SMM 10

Surveys of Modern Mathematics

Finite Groups: An Introduction

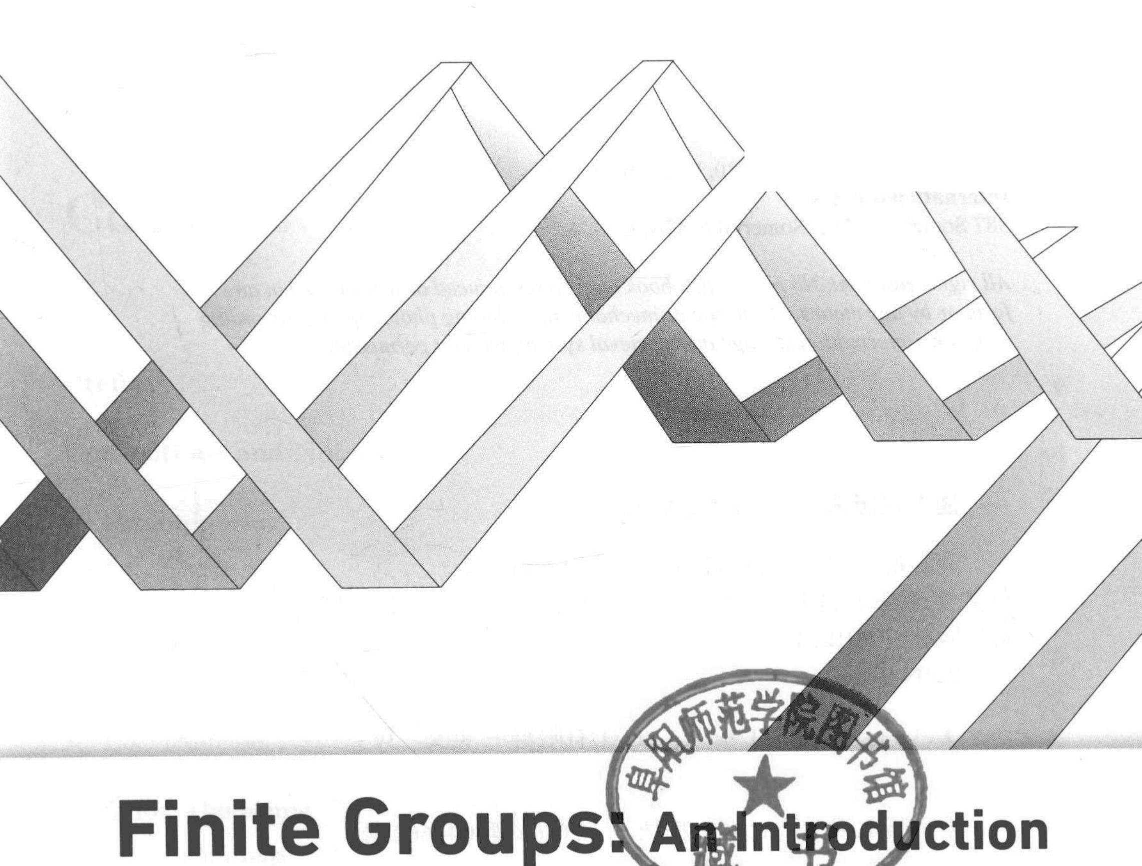
有限群导引

Jean-Pierre Serre



SMM 10

Surveys of Modern Mathematics



Finite Groups: An Introduction

有限群导引

YOUXIANQUN DAOYIN

Jean-Pierre Serre

Translated with the help of Garving K. Luli, Pin Yu

高等教育出版社·北京
HIGHER EDUCATION PRESS BEIJING

International Press

Author
Jean-Pierre Serre
Collège de France

图书在版编目（C I P）数据

有限群导引 = Finite Groups: An Introduction : 英文 / （法）塞尔（Serre, J. P.）著. -- 北京 : 高等教育出版社, 2016. 4
ISBN 978-7-04-044641-8

Ⅰ. ①有… Ⅱ. ①塞… Ⅲ. ①有限群 - 英文 Ⅳ. ① O152.1

中国版本图书馆 CIP 数据核字（2016）第 044662 号

策划编辑 王丽萍　　责任编辑 王丽萍　　封面设计 李小璐　　责任印制 毛斯璐

出版发行	高等教育出版社	网　　址	http://www.hep.edu.cn
社　　址	北京市西城区德外大街4号		http://www.hep.com.cn
邮政编码	100120	网上订购	http://www.hepmall.com.cn
印　　刷	北京中科印刷有限公司		http://www.hepmall.com
开　　本	787mm × 1092mm 1/16		http://www.hepmall.cn
印　　张	12.25		
字　　数	230 千字	版　　次	2016 年 4 月第 1 版
购书热线	010-58581118	印　　次	2016 年 4 月第 1 次印刷
咨询电话	400-810-0598	定　　价	59.00 元

物 料 号 44641-00

Surveys of Modern Mathematics

Surveys of Modern Mathematics

Mathematics has developed to a very high level and is still developing rapidly. An important feature of the modern mathematics is strong interaction between different areas of mathematics. It is both fruitful and beautiful. For further development in mathematics, it is crucial to educate students and younger generations of mathematicians about important theories and recent developments in mathematics. For this purpose, accessible books that instruct and inform the reader are crucial. This new book series "Surveys of Modern Mathematics" (SMM) is especially created with this purpose in mind. Books in SMM will consist of either lecture notes of introductory courses, collections of survey papers, expository monographs on well-known or developing topics.

With joint publication by Higher Education Press (HEP) inside China and International Press (IP) in the West with affordable prices, it is expected that books in this series will broadly reach out to the reader, in particular students, around the world, and hence contribute to mathematics and the world mathematics community.

Series Editors

Preface

This book is based on a course given at École Normale Supérieure de Jeunes Filles, Paris, in 1978-1979. Its aim is to give an introduction to the main elementary theorems of finite group theory.

Handwritten notes were taken by Martine Buhler and Catherine Goldstein (Montrouge, 1979); they were later type-set by Nicolas Billerey, Olivier Dodane and Emmanuel Rey (Strasbourg-Paris, 2004), and made freely available through arXiv:math/0503154. In 2013, they were translated into English by Garving K. Luli and Pin Yu. In 2014-2015, I revised and expanded them (by a factor 2) for the present publication: I gave many references to old and recent results, I added two chapters on finite subgroups of GL_n, and on "small groups", and I also added about 160 exercises.

I thank heartily all the people mentioned above, without whom this book would not have been published.

Jean-Pierre Serre, Paris, Spring 2016

Conventions and Notation

The symbols $\mathbf{Z}, \mathbf{Q}, \mathbf{F}_p, \mathbf{F}_q, \mathbf{R}, \mathbf{C}$ have their usual meaning.

Set theory

If $X \supset Y$, the complement of Y in X is written $X - Y$.

The number of elements of a finite set X is denoted by $|X|$.

Rings

Rings have a unit element, written 1.

If A is a ring, $A^\times$ is the group of invertible elements of A.

The word *field* means *commutative field.*

Group theory

We use standard notation such as $(G : H)$, G/H, $H\backslash G$ when H is a subgroup of a group G.

A group G is abelian (= commutative) if $xy = yx$ for every $x, y \in G$.

If A is a subset of G, the centralizer of A in G is written $C_G(A)$; it is the set of all $g \in G$ such that $ga = ag$ for every $a \in A$. The normalizer of A is written $N_G(A)$; it is the set of all $g \in G$ such that $gAg^{-1} = A$.

If A, B are subsets of G, the set of all products ab with $a \in A$ and $b \in B$ is written either $A.B$ or AB; the subgroup of G generated by A and B is written $\langle A, B\rangle$.

The formula $G = 1$ means that $|G| = 1$; when G is abelian, and written additively, we write $G = 0$ instead.

Symmetric groups

The symmetric and alternating groups of permutations of $\{1, \ldots, n\}$ are written $\mathcal{S}_n$ and $\mathcal{A}_n$. The group of permutations of a set X is written $\mathcal{S}_X$.

Linear groups

If A is a commutative ring, and n is an integer $\geqslant 0$, then:

$\mathrm{M}_n(A) = A$-algebra of $n \times n$ matrices with coefficients in A,

$\mathrm{GL}_n(A) = \mathrm{M}_n(A)^\times =$ group of invertible $n \times n$ matrices with coefficients in A,

$\mathrm{SL}_n(A) = \mathrm{Ker}(\det : \mathrm{GL}_n(A) \to A^\times)$.

We use $\mathrm{End}(V), \mathrm{GL}(V)$ and $\mathrm{SL}(V)$ for the similar notions relative to a vector space of finite dimension.

Let k be a field. If $n \geqslant 1$, there is a natural isomorphism of $k^\times$ onto the center of $\mathrm{GL}_n(k)$; the quotient $\mathrm{GL}_n(k)/k^\times$ is the n-th projective linear group $\mathrm{PGL}_n(k)$.

The image of $\mathrm{SL}_n(k)$ into $\mathrm{PGL}_n(k)$ is denoted by $\mathrm{PSL}_n(k)$.

Contents

Chapter 1

Preliminaries

Let G be a group (finite or infinite). Let us recall a few standard definitions and results relative to G.

1.1 Group actions

Definition 1.1. *A (left) group action of G on a set X is a map*

$$\begin{aligned} G \times X &\longrightarrow X \\ (g, x) &\longmapsto gx \end{aligned}$$

that satisfies the following conditions :

(1) *$g(g'x) = (gg')x$ for all $x \in X$ and all $g, g' \in G$.*

(2) *$1x = x$ for all $x \in X$, where 1 is the identity element of G.*

Note. Right group actions $G \times X \to X$ are defined in a similar way, and denoted by $(x, g) \mapsto xg$. We shall rarely use them. Note that every right action can be replaced by a left one via the recipe : $gx = xg^{-1}$.

Remark. Equivalently, a group action of G on X can be defined as a group homomorphism τ from G to the symmetric group $\mathcal{S}_X$ of X, namely $\tau(g)(x) = gx$ for all $g \in G$ and $x \in X$.

Definition 1.2. *A set X, together with an action of G on it, is called a G-**set**. If X and Y are G-sets, a map $f : X \to Y$ is called a G-**map** if $f(gx) = gf(x)$ for every $g \in G$.*

If X is a G–set, the action of G partitions X into **orbits**: two elements x and y in X are in the same orbit if and only if there exists $g \in G$ such that $x = gy$. The quotient of X by G is the set of orbits and is written X/G (or sometimes $G\backslash X$).

Definition 1.3. *The group G acts transitively on X if X/G consists of only one element.*

In particular, the group G acts transitively on each orbit.

Definition 1.4. *For $x \in X$, the* ***stabilizer*** *of x in G, denoted by G_x, is the subgroup of elements $g \in G$ that fix x (i.e., such that $gx = x$).*

Definition 1.5. *The action of G on X is said to be* ***faithful*** *is $G \to \mathcal{S}_X$ is injective, i.e., if $\bigcap_{x\in X} G_x = 1$. It is said to be* ***free*** *if $G_x = 1$ for every $x \in X$. If G acts freely and transitively, X is called a G-**torsor**.*

Remark. If G acts transitively on X and if $x \in X$, we have a bijection from G/G_x to X given by $gG_x \longmapsto gx$, where G/G_x is the set of left cosets of G_x in G. If $x' \in X$, there exists $g \in G$ such that $x' = gx$. Thus, $G_{x'} = gG_xg^{-1}$. In other words, changing x amounts to replacing its stabilizer by a conjugate. Conversely, if H is a subgroup of G, then G acts transitively on G/H and H fixes the class of 1. Therefore, giving a set X on which G acts transitively amounts to giving a subgroup of G, up to conjugation.

Example. Let K be a field, and let G be the group of automorphisms of the set K defined by :

$$G = \left\{x \mapsto ax + b,\ a \in K^\times,\ b \in K\right\}.$$

Then G acts transitively on K. If $x_0 \in K$, the stabilizer of x_0 is the group of homotheties centered at x_0, namely $x \mapsto x_0 + a(x - x_0)$, $a \in K^\times$; it is isomorphic to $K^\times$.

Application. Suppose that G is finite and let $|G|$ denote its order. If X is a finite G-set, we have $X = \bigcup_{i\in I} Gx_i$, where the Gx_i are the pairwise disjoint orbits under the action of G and x_i is a representative element from each orbit. We have $|Gx_i| = |G|.\,|G_{x_i}|^{-1}$. Hence

$$|X| = \sum_{i\in I}(G : G_{x_i}) = |G|\sum_{i\in I}\frac{1}{|G_{x_i}|}. \tag{1.1}$$

Inner automorphisms and conjugacy classes. Let $g \in G$. The map $\mathrm{int}_g : x \mapsto gxg^{-1}$ is an automorphism of G, which is called the **inner automorphism** defined by g. The map $g \mapsto \mathrm{int}_g$ is a homomorphism of G into the automorphism group $\mathrm{Aut}(G)$ of G. It defines an action of G on itself; the orbits of that action are the **conjugacy classes** of G. The stabilizer of an element x of G is the set of elements of G that commute with x, i.e., the **centralizer** of x; we denote it by $C_G(x)$. We have

$$1 = \sum_{i=1}^{h}\frac{1}{|C_G(x_i)|}, \tag{1.2}$$

where h is the number of conjugacy classes, and the x_i are representatives of these classes. In this equation the largest value of $|C_G(x_i)|$ is $|G|$; this fact can be used to obtain an upper bound for $|G|$ when h is known, cf. exerc.7.

Counting orbits.

The following result is usually called **Burnside's lemma**, even though it had already been published before Burnside by Cauchy and later by Frobenius:

Proposition 1.1. *Let G be a finite group and let X be a finite G-set. For every $g \in G$, let $X^g \subset X$ be the set of elements x of X which are fixed under the action of g, and let $\chi_X(g) = |X^g|$. Then :*

$$|X/G| = \frac{1}{|G|}\sum_{g\in G}\chi_X(g). \tag{1.3}$$

[In other words, the number of orbits is the average of the number of fixed points of the elements of the group.]

Proof. By splitting X into orbits, we may assume that G acts transitively, hence that $X = G/H$, where H is a subgroup of G. If $(g,x) \in G \times X$, define $f(g,x)$ to be equal to 1 if $gx = x$, and to 0 if $gx \neq x$. Let us compute in two different ways the sum $S = \sum_{(g,x)\in G\times X} f(g,x)$:

i) For $x \in X$, the sum $\sum_{g\in G} f(g,x)$ is the number of elements of G which fix x, i.e., $|H|$. Hence $S = |X|\,|H| = |G|$.

ii) For $g \in G$, the sum $\sum_{x\in X} f(g,x)$ is the number of elements of X fixed by g, i.e., $\chi_X(g)$. Hence $S = \sum_{g\in G}\chi_X(g)$.

By comparing the two formulas, we obtain $|G| = \sum_{g\in G}\chi_X(g)$, which is equivalent to (1.3) since $|X/G| = 1$.

1.2 Normal subgroups, automorphisms, characteristic subgroups, simple groups

Recall that a subgroup H of G is **normal** if, for all $x \in G$ and all $h \in H$, we have $xhx^{-1} \in H$. This means that H is stable under the inner automorphisms of G. The quotient G/H has a unique group structure such that $G \to G/H$ is a homomorphism, and we have the exact sequence:

$$1 \longrightarrow H \longrightarrow G \longrightarrow G/H \longrightarrow 1\,.$$

Note. A sequence of group homomorphisms $\cdots \to G_i \to G_{i+1} \to \cdots$ is said to be **exact** if, for every i, the kernel of $G_i \to G_{i+1}$ is equal to the image of $G_{i-1} \to G_i$.

Example. The inner automorphisms $\{\mathrm{int}_g\}_{g\in G}$ make up a normal subgroup $\mathrm{Int}(G)$ of the group $\mathrm{Aut}(G)$ of all the automorphisms of G. The quotient $\mathrm{Out}(G) = \mathrm{Aut}(G)/\mathrm{Int}(G)$ is the **outer automorphism group** of G. We thus have exact sequences :

$$1 \to Z(G) \to G \to \mathrm{Int}(G) \to 1 \quad \text{and} \quad 1 \to \mathrm{Int}(G) \to \mathrm{Aut}(G) \to \mathrm{Out}(G) \to 1,$$

where $Z(G) = C_G(G)$ is the **center** of G.

If H is a normal subgroup of a group G, the action of G on H by inner automorphisms defines a homomorphism $G \to \mathrm{Aut}(H)$; this homomorphism maps H onto $\mathrm{Int}(H)$, hence defines a map: $G/H \to \mathrm{Out}(H)$.

Proposition 1.2. *Let M and N be two normal subgroups of G such that $M \cap N = 1$. Then M and N commute elementwise, i.e., $xy = yx$ for every $x \in M$ and $y \in N$.*

Indeed, the element $x\,yx^{-1}y^{-1} = xyx^{-1}\,y^{-1}$ belongs to both M and N, hence is equal to 1.

Definition 1.6. *A subgroup H of G is* **characteristic** *if it is stable under every automorphism of G.*

Such a subgroup is normal in G. More generally, if $H \subset N \subset G$, with H is characteristic in N, and N normal in G, then H is normal in G.

Examples. The **center** $Z(G) = C_G(G)$ of G is a characteristic subgroup. The **derived group** of G is characteristic, and so are the subgroups D^nG, C^iG and $\Phi(G)$ defined in chap.3.

Definition 1.7. *A group G is* ***simple*** *if the number of its normal subgroups is 2. Equivalently, $G \neq 1$, and the only normal subgroups of G are 1 and G.*

Examples.

1. The abelian simple groups are the cyclic groups of prime order, i.e., the groups $\mathbf{Z}/p\mathbf{Z}$ for some prime p.

2. The alternating subgroup $\mathcal{A}_n$ is simple abelian if $n = 3$, and simple nonabelian if $n \geqslant 5$, cf. exerc.19, or Huppert [25], p.156, Satz 2.4, or Lang [29], chap.I, th. 5.5.

3. If K is a field, the group $\mathbf{PSL}_n(K)$ is simple for $n \geqslant 2$, except when $n = 2$ and $|K| = 2$ or 3, cf. chap.3, exerc.7, or Huppert [25], p.182, Satz 6.13, or Lang [29], chap.XIII, §8 and §9.

4. A nonabelian simple group of order < 200 has order either 60 or 168; it is isomorphic to either $\mathcal{A}_5$ or $\mathrm{SL}_3(\mathbf{F}_2)$, cf. §7.7.

For more information on the structure of the finite simple groups, including the *sporadic* ones, see Gorenstein [21], Gorenstein-Lyons-Solomon [22] and Wilson [39]. The reader will find in these books a precise statement of the *Classification of Finite Simple Groups* (CFSG), and of its many remarkable consequences (see especially [21], §1.7). Whether this statement is presently a theorem is not clear. The only detailed proof is that of the series [22], and it is not complete yet.

In this book, when we quote a result which depends on CFSG, we state this dependence explicitly.

1.3 Filtrations and Jordan-Hölder theorem

Definition 1.8. *A* ***filtration*** *of a group G is a sequence of subgroups $(G_i)_{0\leqslant i\leqslant n}$ such that*

$$G_0 = G \supset G_1 \supset \cdots \supset G_i \supset \cdots \supset G_n = 1, \tag{1.4}$$

with G_{i+1} normal in G_i, for $i = 1, \ldots, n-1$. Given a filtration $(G_i)_{0\leqslant i\leqslant n}$, the successive quotients $G_i/G_{i+1}, 0 \leqslant i < n$, are denoted by $\mathrm{gr}_i(G)$. The sequence of the $\mathrm{gr}_i(G)$ is denoted by $\mathrm{gr}(G)$.

Remark. There are several variants of the above definition: one may use infinite filtrations, or filtrations beginning with G_1 intead of G_0, or filtrations not ending with 1, etc.

Definition 1.9. *A filtration $(G_i)_{0\leqslant i\leqslant n}$ of G is called a* ***Jordan-Hölder filtration*** *(or a* ***Jordan-Hölder series*** *or a* ***composition series****) if $\mathrm{gr}_i(G) = G_i/G_{i+1}$ is simple for every i such that $0 \leqslant i < n$. The number n is called the* ***length*** *of the filtration.*

Proposition 1.3. *Every finite group has a Jordan-Hölder filtration.*

Proof. If $G = 1$, take the trivial Jordan-Hölder filtration with $n = 0$ in (1.4); if G is simple, take $n = 1$ in (1.4). Suppose that G is neither 1 nor simple. Use induction on the order of G. Let N be a normal subgroup of G, distinct from G, and of maximal order. Then G/N is simple. Since $|N| < |G|$, we apply the induction hypothesis to N and we obtain a Jordan-Hölder filtration (N_i) for N. Then $(G, N_0, N_1, \ldots)$ is a Jordan-Hölder filtration for G.

Remark. An infinite group may not have a Jordan-Hölder filtration; example: $\mathbf{Z}$.

Theorem 1.4 (Jordan-Hölder). *Let $(G_i)_{0\leqslant i\leqslant n}$ be a Jordan-Hölder filtration of a group G. Then the $\mathrm{gr}_i(G)$ (the successive factor groups) do not depend on the choice of the filtration, up to permutation of the indices. In particular, the length of the filtration is independent of the filtration.*

[The length of the filtration is called the *length of* G, and is denoted by $\ell(G)$; when G has no Jordan-Hölder filtration, we write $\ell(G) = \infty$.]

Proof.

Let S be a simple group, and let $n(G, (G_i), S)$ be the number of j such that G_j/G_{j+1} is isomorphic to S. What we have to prove is that $n(G, (G_i), S)$ does not depend on the chosen filtration (G_i).

Note first that, if H is a subgroup of G, a filtration (G_i) of G induces a filtration (H_i) of H by putting $H_i = G_i \cap H$.

Similarly, if N is a normal subgroup of G, we obtain a filtration of G/N by putting $(G/N)_i = G_i/(G_i \cap N) = G_iN/N$. The exact sequence $1 \to N \to G \to G/N \to 1$ gives an exact sequence

$$1 \to N_i/N_{i+1} \to G_i/G_{i+1} \to (G/N)_i/(G/N)_{i+1} \to 1,$$

i.e.,

$$1 \to \mathrm{gr}_i(N) \to \mathrm{gr}_i(G) \to \mathrm{gr}_i(G/N) \to 1.$$

If (G_i) is a Jordan-Hölder filtration, all the $\mathrm{gr}_i(G)$ are simple; thus, $\mathrm{gr}_i(N)$ is either 1 or $\mathrm{gr}_i(G)$. Let us partition $I = \{1, \dots, n\}$ into two sets:

$$I_1 = \{i \in I,\, \mathrm{gr}_i(N) = \mathrm{gr}_i(G)\} \quad \text{and} \quad I_2 = \{i \in I,\, \mathrm{gr}_i(N) = 1\}.$$

By reindexing I_1 (resp. I_2) we obtain a Jordan-Hölder filtration of N (resp. of G/N) of length $|I_1|$ (resp. of length $|I_2|$); note that $|I_1| + |I_2| = n$.

We now prove the theorem by induction on the length n of the filtration (G_i). If $n = 0$, then $G = 1$, and if $n = 1$, then G is simple and only one filtration is possible. Assume that $n \geqslant 2$, i.e., that G is neither 1 nor simple. Choose a normal subgroup N of G distinct from 1 and G. The sets I_1 and I_2 defined above are not empty, hence their number of elements is $< n$, and we can apply the induction hypothesis to N and G/N; it shows that $n(N, (N_i)_{i\in I_1}, S)$ and $n(G/N, ((G/N)_i)_{i\in I_2}, S)$ are independent of the filtrations. Since

$$n(G, (G_i)_{i\in I}, S) = n(N, (N_i)_{i\in I_1}, S) + n(G/N, ((G/N)_i)_{i\in I_2}, S),$$

this implies that $n(G, (G_i)_{i\in I}, S)$ is independent of the choice of filtration, as wanted.

Corollary 1.5. *If N is a normal subgroup of G, then $\ell(G) = \ell(N) + \ell(G/N)$.*

This has been proved in the argument above when $\ell(G) < \infty$. When $\ell(G) = \infty$, then the same is true for either N or G/N, and we still have $\ell(G) = \ell(N) + \ell(G/N)$.

Application. A special case of the Jordan-Hölder theorem is the uniqueness of the prime factorization of an integer $n \geqslant 1$. Indeed, if $n = p_1^{h_1} \cdots p_k^{h_k}$, we have the following Jordan-Hölder filtration for $\mathbf{Z}/n\mathbf{Z}$:

$$\mathbf{Z}/n\mathbf{Z} \supset p_1\mathbf{Z}/n\mathbf{Z} \supset p_1^2\mathbf{Z}/n\mathbf{Z} \supset \cdots \supset p_1^{h_1}\mathbf{Z}/n\mathbf{Z} \supset p_1^{h_1}p_2\mathbf{Z}/n\mathbf{Z} \supset p_1^{h_1}p_2^2\mathbf{Z}/n\mathbf{Z} \supset \cdots$$

The factor group $\mathbf{Z}/p_i\mathbf{Z}$ appears h_i times; thus, uniqueness follows.

Examples.

1. Filtration of $\mathcal{S}_3$: there is a unique Jordan-Hölder filtration:

$$\mathcal{S}_3 \supset \mathcal{A}_3 \supset 1,$$

where the successive quotients are cyclic of order 2 and 3.

2. Filtration of $\mathcal{S}_4$: the alternating group $\mathcal{A}_4$ is a normal subgroup of $\mathcal{S}_4$ of index 2. Let $D = \{1, \sigma_1, \sigma_2, \sigma_3\}$ with[1]

$$\begin{aligned}\sigma_1 &= (1\ 2)(3\ 4),\\ \sigma_2 &= (1\ 3)(2\ 4),\\ \sigma_3 &= (1\ 4)(2\ 3).\end{aligned}$$

The group D is elementary abelian of type (2,2) (i.e., it is a direct product of two groups of order 2). It is a normal subgroup of $\mathcal{A}_4$ and we have the Jordan-Hölder filtration:

$$\mathcal{S}_4 \supset \mathcal{A}_4 \supset D \supset \{1, \sigma_i\} \supset 1. \tag{1.5}$$

The orders of the successive quotients are $2, 3, 2, 2$. The filtration is not unique since the index i in (1.5) can be chosen to be 1, 2 or 3.

3. Filtration of $\mathcal{S}_n$, $n \geqslant 5$: the subgroup $\mathcal{A}_n$ is simple, see exerc.19. There is a unique Jordan-Hölder filtration:

$$\mathcal{S}_n \supset \mathcal{A}_n \supset 1.$$

The orders of the successive quotients are 2 and $\frac{1}{2}n!$.

Generalization to groups with operators. Everything we have done in the present section extends without any change to *groups with operators*, i.e., to groups G endowed with a family Φ of endomorphisms $\varphi : G \to G$, cf. e.g., Bourbaki [3], §4.7. In that setting, the subgroups should be replaced by the Φ- subgroups, i.e., the subgroups stable under all $\varphi \in \Phi$; a Φ-group is called simple if the number of its normal Φ-subgroups is equal to 2; a Jordan-Hölder filtration is defined in an obvious way. The point of this generalization is that *it applies to the category of A-modules* (s, say), with $\Phi = A$ acting by homotheties. Hence it makes sense to speak of a *simple A-module*, or a module *of finite length*. We shall see some examples of this in chapter 8.

1.4 Subgroups of products: Goursat's lemma and Ribet's lemma

We give here two results which, although easy to prove, are useful in Galois theory. Both of them are about subgroups of a direct product $G_1 \times \cdots \times G_n$ and their behavior with respect to the projection maps $\mathrm{pr}_i : G_1 \times \cdots \times G_n \to G_i$.

In the first one, $n = 2$. It describes the subgroups H of $G_1 \times G_2$ such that $\mathrm{pr}_1(H) = G_1$ and $\mathrm{pr}_2(H) = G_2$: they correspond to isomorphisms between a quotient of G_1 and a quotient of G_2. More precisely:

[1] We use here the standard notation where $(a_1\ a_2\ \ldots\ a_m)$ means the cyclic permutation $a_1 \mapsto a_2$, $a_2 \mapsto a_3$, …, $a_m \mapsto a_1$. In particular, $(a\ b)$ means the transposition of a and b.

Proposition 1.6 (Goursat's lemma). *For $i = 1, 2$, let N_i be a normal subgroup of G_i and let $\varphi : G_1/N_1 \to G_2/N_2$ be an isomorphism. Let $H_{N_1,N_2,\varphi}$ be the set of all $(g_1, g_2) \in G_1 \times G_2$ which are such that $\varphi(\overline{g_1}) = \overline{g_2}$, where $\overline{g_i}$ is the image of g_i in G_i/N_i. Then :*

i) $\mathrm{pr}_i(H_{N_1,N_2,\varphi}) = G_i$ *for $i = 1, 2$.*

ii) Every subgroup H of $G_1 \times G_2$ such that $\mathrm{pr}_i(H) = G_i$ *for $i = 1, 2$ is equal to some $H_{N_1,N_2,\varphi}$ for a unique choice of N_1, N_2 and φ.*

[Note that $H_{N_1,N_2,\varphi}$ may be viewed as a kind of *graph* of φ.]

Proof of i). Let g_1 be an element of G_1. Choose $g_2 \in G_2$ such that $\overline{g_2} = \varphi(\overline{g_1})$, and let $h = (g_1, g_2)$. We have $h \in H$ and $\mathrm{pr}_1(h) = g_1$. Same argument for pr_2, with φ replaced by φ^{-1}.

Proof of ii). Define N_1 as $H \cap G_1$, where G_1 is viewed as a subgroup of $G_1 \times G_2$, namely the kernel of pr_2. Define similarly $N_2 = H \cap G_2$. By assumption, we have $H.G_1 = G_1 \times G_2$, since both H and G_2 normalize H and G_1, this shows that $G_1 \times G_2$ normalizes N_1, i.e., that N_1 is normal in G_1. Similarly N_2 is normal in G_2. Moreover, we have natural isomorphisms:

$$G_1/N_1 \simeq H/(N_1 \times N_2) \simeq G_2/N_2.$$

This defines an isomorphism $\varphi : G_1/N_1 \to G_2/N_2$, and it is clear that the corresponding $H_{N_1,N_2,\varphi}$ is equal to H. The uniqueness of the construction is also clear.

Corollary 1.7. *Assume that no quotient of G_1 distinct from 1 is isomorphic to a quotient of G_2. Then the only subgroup H of $G_1 \times G_2$ such that* $\mathrm{pr}_i(H) = G_i$ *for $i = 1, 2$ is $H = G_1 \times G_2$.*

Galois interpretation

In Galois theory, the situation of Goursat's lemma arises as follows. We have two Galois extensions L_1/K and L_2/K of the same field K, which are embedded in a Galois extension L/K in such a way that $L = L_1.L_2$. Let $G_i, i = 1, 2$, be the Galois group of L_i/K and let H be the Galois group of L/K. The natural maps $H \to G_1$ and $H \to G_2$ give an embedding of H into $G_1 \times G_2$; hence we may view H as a subgroup of $G_1 \times G_2$. Let M be $L_1 \cap L_2$. The group N_1 introduced in the above proof is $\mathrm{Gal}(L_1/M) \simeq \mathrm{Gal}(L/L_2)$; similarly, $N_2 = \mathrm{Gal}(L_2/M) \simeq \mathrm{Gal}(L/L_1)$, and we have $\mathrm{Gal}(L/M) = N_1 \times N_2$ and $\mathrm{Gal}(M/K) \simeq H/(N_1 \times N_2) \simeq G_1/N_1 \simeq G_2/N_2$.
The group H is equal to $G_1 \times G_2$ if and only if $L_1 \cap L_2 = K$, in which case $L \simeq L_1 \otimes_K L_2$.

Ribet's lemma

The second result is about $n \geqslant 2$ and the projections $\mathrm{pr}_{ij} : G_1 \times \cdots \times G_n \to G_i \times G_j$.

Proposition 1.8 (Ribet). *Let H be a subgroup of $G_1 \times \cdots \times G_n$.*
Assume that $\mathrm{pr}_{ij}(H) = G_i \times G_j$ for every i, j, and that the G_i, with at most two exceptions, can be generated by commutators (i.e., elements of the form $xyx^{-1}y^{-1}$). *Then $H = G_1 \times \cdots \times G_n$.*

Proof. Use induction on n, starting with $n = 2$, which is obvious.
Suppose that $n \geqslant 3$. We may suppose that G_1 is generated by commutators. The induction assumption shows that the projection $H \to G_2 \times \cdots \times G_n$ is surjective. Hence we only have to show that H contains G_1. Because of the assumption made on G_1, it is enough to prove that, if x, y are two elements of G_1, then $xyx^{-1}y^{-1}$ belongs to H. Since $\mathrm{pr}_{1n}(H) = G_1 \times G_n$, there exists $u \in G_2 \times \cdots \times G_{n-1}$ with $(x, u, 1) \in H$. The induction assumption shows that $H \to G_1 \times \cdots \times G_{n-1}$ is surjective; hence there exists $v \in G_n$ such that $(y, 1, v) \in H$. We then have

$$(xyx^{-1}y^{-1}, 1, 1) = (x, u, 1).(y, 1, v).(x, u, 1)^{-1}.(y, 1, v)^{-1},$$

which shows that $(xyx^{-1}y^{-1}, 1, 1)$ belongs to H.

1.5 Exercises

1. (*Commutativity criteria.*) Let G be a group. Show the equivalence of the following properties of G:
   a) The map $x \mapsto x^{-1}$ is an automorphism of G.
   b) The diagonal of $G \times G$ is a normal subgroup of $G \times G$.
   c) The map $(x, y) \mapsto xy$ is a homomorphism of $G \times G$ into G.
   d) $G/Z(G)$ is cyclic.
   e) G is abelian.

2. Let G be a group. Show that $\mathrm{Aut}(G) = 1 \Longleftrightarrow |G| \leqslant 2$.

3. Let H be a subgroup of finite index n of a group G. Show that $g \in Z(G) \Longrightarrow g^n \in H$.
   [Hint: Let C be the subgroup of G generated by g. Use the fact that $C/C \cap H$ acts freely on G/H, hence $(C : C \cap H)$ divides n.]

4. Let G be a group.
   a) Let X, Y be two G-sets, let $x \in X$ and let $y \in Y$. Assume that, for every $g \in G$, either x or y is fixed under the action of g. Show that one the points x, y is fixed by G.
   [Hint: suppose not; choose $g, h \in G$ such that $gx \neq x$ and $hy \neq y$; show that $ghx \neq x$ and $ghy \neq y$: contradiction.]
   b) Let H, H' be two proper subgroups of G. Show that $G \neq H \cup H'$.
   Give an example of a group which is the union of three proper subgroups.

5. Let G be a group and let H be a subgroup of G of finite index n. Let H' be the intersection of the conjugates of H in G. Show that G/H' is isomorphic to a subgroup of $\mathcal{S}_n$, hence $(G : H')$ divides $n!$ In particular, if $n = 2$, then $H' = H$; if $n = 3$, then $H' = H$ or $(H : H') = 3$.

6. (*Variations on Wilson's theorem.*) Let G be a finite abelian group and let G_2 be the set of elements of G of order 2.
a) Define $z \in G$ by $z = \prod_{g \in G} g$. Show that $z = \prod_{g \in G_2} g$. Deduce that $z = 1$ if $|G_2| \neq 1$ and that z is the only element of G_2 if $|G_2| = 1$.
b) Take $G = \mathbf{F}_p^\times$ with p prime $\neq 2$. Use a) to show that $(p-1)! \equiv -1 \pmod{p}$ (Wilson's theorem).
c) Let $m = (p-1)/2$; let t be the reduction of $m!$ mod p. Show that $t^2 = (-1)^{m+1}$. Suppose that m is odd, so that $t = \pm 1$. Let $n(p)$ be the number of integers i with $1 \leqslant i \leqslant m$ which are nonsquares mod p. Show that $t = (-1)^{n(p)}$.
[Hint: Let N (resp. N') be the set of elements of $[1, m]$ which are nonsquares (resp. squares) mod p. Identify N and N' with their images in $G = \mathbf{F}_p^\times$. An element x of G is a square if and only if either $x \in N'$ or $-x \in N$. Use (a) to show that $\prod_{x \in N'} x \prod_{y \in N} (-y) = 1$; hence $t = \prod_{x \in N'} x \prod_{y \in N} y = (-1)^{n(p)}$.]

[When $p \equiv 3 \pmod 4$ and $p > 3$, one can show that $n(p)$ is odd if and only if the class number $h(-p)$ is $\equiv 1 \pmod 4$), see e.g. Cohen [15], exerc.43 of chap.11.]

7. (*Upper bound for $|G|$ in terms of the number of conjugacy classes.*)
(a) Let x be a positive rational number, and let h be an integer $\geqslant 1$. Show that there are only a finite number of families $(n_1, \ldots, n_h)$ of integers $\geqslant 1$ such that $\sum_{i=1}^h 1/n_i = x$.
[Hint: note that the smallest n_i is $\leqslant x/h$, hence can only take finitely many values; conclude by using induction on h.]
(b) Show that, if G is a finite group with h conjugacy classes, then $|G|$ is bounded by a function of h.
[Hint: use (a), applied to formula (1.2); note that the largest n_i is equal to $|G|$.]

[Effective upper bounds for $|G|$ can be found in Erdös & Turán [51], Pyber [71] and Keller [63].]

8. Let G be a finite group; let n be its order and let h be the number of its conjugacy classes. Let C be the subset of $G \times G$ made up of the pairs (x, y) such that $xy = yx$. Show that $|C| = nh$.

9. (*A variant of Goursat's lemma.*) Let $f_1 : G \to G_1$ and $f_2 : G \to G_2$ be two homomorphisms of a group G into two groups G_1 and G_2. Assume that each f_i is surjective but that $(f_1, f_2) : G \to G_1 \times G_2$ is not. Show that there exists a nontrivial group A, together with surjective homomorphisms $p_1 : G_1 \to A$ and $p_2 : G_2 \to A$ such that $p_1 \circ f_1 = p_2 \circ f_2$.
[Hint: apply prop. 1.6 with H equal to the image of $(f_1, f_2) : G \to G_1 \times G_2$.]

10. (*Simple groups occurring in a given group.*) Let S be a simple group, and let G be a group. We say that S **occurs** [2] in G if there exist subgroups H and N of G, with N normal in H, such that $H/N \simeq S$. The set of isomorphy classes of simple groups occurring in G is denoted by $\mathrm{Occ}(G)$.
a) Show that, if $G' \subset G$, then $\mathrm{Occ}(G') \subset \mathrm{Occ}(G)$, and, if N is normal in G, then:

[2] Another terminology is : *S is involved in G*.

$$\mathrm{Occ}(G) = \mathrm{Occ}(N) \cup \mathrm{Occ}(G/N).$$

b) Show that $\mathrm{Occ}(G) = \varnothing \Longleftrightarrow G = 1$.
c) Let G_1 and G_2 be two groups such that $\mathrm{Occ}(G_1) \cap \mathrm{Occ}(G_2) = \varnothing$. Show that the only subgroups of $G_1 \times G_2$ are the products $H_1 \times H_2$, with $H_i \subset G_i$ for $i = 1, 2$.
[Hint: apply Goursat's lemma and b).]

11. (*2-transitivity.*) Let G be a group acting on a set X with $|X| \geqslant 2$. The action of G is said to be **2-transitive** if G acts transitively on $X \times X - \Delta$, where Δ is the diagonal of $X \times X$. Equivalently:

(i) For every $x_1, y_1, x_2, y_2 \in X$, with $x_i \neq y_i$ for $i = 1, 2$, there exists $g \in G$ such that $gx_i = y_i$ for $i = 1, 2$.

(ii) The action of G on X is transitive and, if $H \subset G$ is the stabilizer of a point x of X, the action of H on $X - \{x\}$ is transitive.

(iii) The number of orbits of G acting on $X \times X$ is 2.

Suppose that G and X are finite. Show that these properties are also equivalent to :

(iv) $\frac{1}{|G|} \sum_{g \in G} \chi_X(g)^2 \leqslant 2$, where $\chi_X(g) = |X^g|$ as in prop.1.1.

(v) $\frac{1}{|G|} \sum_{g \in G} \chi_X(g)^2 = 2$.

[Hint for (iv) and (v): apply prop.1.1 to $X \times X$ and observe that $\chi_{X \times X}(g) = \chi_X(g)^2$.]

12. Let n be an integer $\geqslant 0$, let X be a set with $|X| \geqslant n$, and let X^n be the product of n copies of X. If $x = (x_1, \ldots, x_n)$ is a point of X^n, let R_x be the equivalence relation on $\{1, \ldots, n\}$ defined by $i \equiv j \Longleftrightarrow x_i = x_j$. The group $\mathcal{S}_X$ acts in an obvious way on X^n. Show that two points x, y of X^n are in same $\mathcal{S}_X$-orbit if and only if $R_x = R_y$. Conclude that the number of these orbits is equal to the number $B(n)$ of equivalence relations on the set $\{1, \ldots, n\}$; this number is called the *n-th Bell number*, cf. Stanley [38], pp. 33-34. Prove the recurrence formula $B(n+1) = \sum_{k=0}^{k=n} \binom{n}{k} B(k)$, and use it to compute the first values of $B(n)$, namely: 1, 1, 2, 5, 15, ...

13. (*n-transitivity.*) Let n be an integer $\geqslant 2$, and let G be a group acting on a set X with $|X| \geqslant n$. Let X^n be the product of n copies of X, and let $X^n_{\mathrm{dist}} \subset X^n$ be the set of n-tuples $(x_1, \ldots, x_n)$ made up of distinct elements. The action of G on X is said to be **n-transitive** if:

(i-n) G acts transitively on X^n_{dist}.

(For $n = 2$ this reduces to the definition given in exerc.11.)
Show that (i-n) is equivalent to each of the following conditions:

(ii-n) The action of G on X is transitive and, if $H \subset G$ is the stabilizer of a point x of X, the action of H on $X - \{x\}$ is $(n-1)$-transitive.

(ii′-n) The orbits of G on X^n are the same as those of $\mathcal{S}_X$.

(iii-n) The number of orbits of G on X^n is $B(n)$, where $B(n)$ is the n-th Bell number, cf. exerc.12.

When G and X are finite, prove the equivalence of these conditions with:

(iv-n) $\frac{1}{|G|} \sum_{g \in G} \chi_X(g)^n \leqslant B(n)$, where $\chi_X(g) = |X^g|$.

(v-n) $\frac{1}{|G|}\sum_{g\in G}\chi_X(g)^n = B(n)$.

14. Let G be a group and let X and Y be two finite G-sets. If H is a subgroup of G, let X^H and Y^H be the subsets of X and Y fixed under H. Show that, if $|X^H| = |Y^H|$ for every H, then X and Y are isomorphic.
[Hint: Use induction on $|X|$. Let Ω be the set of subgroups of G which are the stabilizers of the points of X; choose $H \in \Omega$ such that $(G : H)$ is minimal. Then, if H' contains H, we have $|X^{H'}| > 0$ if and only if $H' = H$. Hence the same is true for $|Y^{H'}|$; in particular, there exists a point of Y whose stabilizer is H. This shows that X and Y are isomorphic to the disjoint union of G/H and two G-sets X' and Y'. Apply the induction hypothesis to X' and Y'.]

15. Let G be a finite group of order $\geqslant 3$. Assume that $\mathrm{Aut}(G)$ acts transitively on the set $G - \{1\}$.
a) Show that there exists a prime number p such that every element of $G - \{1\}$ has order p.
b) If $p = 2$, show that G is a direct product of groups of order 2.
c) If $p > 2$, and if the action of $\mathrm{Aut}(G)$ on $G - \{1\}$ is 2-transitive, show that $|G| = 3$.
[Hint: If not, choose $x, y \in G - \{1\}$ such that $y \neq x, x^{-1}$; no automorphism of G can map the pair (x, y) onto the pair (x, x^{-1}).]
d) Assume that $|G| \geqslant 4$ and that $\mathrm{Aut}(G)$ acts 3-transitively on $G - \{1\}$. Show that $|G| = 4$.

16. (*Primitive actions.*) Let X be a G-set on which G acts transitively, with $|X| \geqslant 2$, and let H be the stabilizer of a point of X. The action of G is said to be **primitive** if H is **maximal**, i.e., is maximal among the proper subgroups of G. Show that this is equivalent to the following property:
Every G-map of X into another G-set is either injective or trivial (= image reduced to one point).
Show that a 2-transitive action is primitive.

17. (*Simplicity of $\mathcal{A}_5$.*) Let $G = \mathcal{A}_5$. Show that it has 5 conjugacy classes containing respectively 1, 12, 12, 15 and 20 elements. Let H be a subset of G, stable under inner conjugation, containing 1 and distinct from 1 and G; it is a union of conjugacy classes; check that $|H|$ is equal to 13, 16, 21, 25, 28, 33, 36, 40, 45 or 48. Since none of these numbers divide 60, conclude that H is not a subgroup of G. Hence G is simple.

18. (*Automorphism groups of $\mathcal{A}_5$, $\mathcal{A}_4$ and $\mathcal{S}_4$.*) Let $G = \mathcal{A}_5$.
a) Let $x = (1\ 2)(3\ 4) \in G$. Let y be an element of G of order 3; show that xy has order 5 if and only if the set of fixed points of y meets both $\{1, 2\}$ and $\{3, 4\}$.
b) Let X be the set of pairs $u, v \in G$ such that u has order 2, v has order 3, and uv has order 5. Show that $|X| = 120$.
[Hint: show that the number of elements u of order 2 is 15, and for a given u, use a) to prove that the number of possible v is 8. Alternate method: use formula (8.27) of chap.8.]
c) The group $\mathrm{Aut}(G)$ acts on X. Show that this action is free.
[Hint: prove first that, if (u, v) belongs to X, then (u, v) generate G.]
Deduce that $|\mathrm{Aut}(G)| \leqslant 120$; since $\mathrm{Aut}(G)$ contains $\mathcal{S}_5$, conclude that $\mathrm{Aut}(G) = \mathcal{S}_5$.

d) Use a similar argument, with $(2,3,5)$ replaced by $(2,3,4)$, to show that $\mathrm{Aut}(\mathcal{A}_4) = \mathcal{S}_4$.
e) Use a similar argument, with $(2,3,5)$ replaced by $(2,3,3)$, to show that $\mathrm{Aut}(\mathcal{S}_4) = \mathcal{S}_4$.
[Alternate method: deduce it from d).]

19. (*Simplicity of $\mathcal{A}_n$ for $n \geqslant 6$.*) Let $X = \{1,\dots,n\}$, where n is an integer $\geqslant 6$. The subgroup of $\mathcal{A}_n$ fixing n is $\mathcal{A}_{n-1}$; assume that this subgroup is simple.
a) Show that $\mathcal{A}_{n-1}$ is a maximal subgroup of $\mathcal{A}_n$.
[Hint: use the fact that the action of $\mathcal{A}_n$ on X is 2-transitive.]
b) Let N be a normal subgroup of $\mathcal{A}_n$ distinct from 1 and $\mathcal{A}_n$. Show that $N \cap \mathcal{A}_{n-1} = 1$ and that $N\mathcal{A}_{n-1} = \mathcal{A}_n$. Hence $|N| = n$.
c) Let $\varphi : N \to X$ be the map given by $\varphi(g) = g(n)$. Show that φ is bijective. Show that φ is compatible with the action of $\mathcal{A}_{n-1}$ on N (by conjugation) and on X, i.e., that $\varphi(hxh^{-1}) = h\varphi(x)$ if $h \in \mathcal{A}_{n-1}$ and $x \in N$.
d) Use c) to show that the map $\mathcal{A}_{n-1} \to \mathrm{Aut}(N)$ given by conjugation is an isomorphism of $\mathcal{A}_{n-1}$ on the group of even permutations of the set $N - \{1\}$. Use exerc.15 to show that this is impossible. Hence $\mathcal{A}_n$ is simple.
This gives an inductive proof of the simplicity of $\mathcal{A}_n$ for $n \geqslant 5$, starting with the case of $\mathcal{A}_5$, see exerc.17.

20. Let K be a field, and n be an integer $\geqslant 2$. Show that $\mathrm{PGL}_n(K)$ has finite length if and only if $K^\times/K^{\times n}$ is finite.
[Hint: use the exact sequence $1 \to \mathrm{PSL}_n(K) \to \mathrm{PGL}_n(K) \to K^\times/K^{\times n} \to 1$, together with the simplicity of $\mathrm{PSL}_n(K)$, when K is infinite, cf. chap.3, exerc.7.]

21. (*How to generate (or not generate) the symmetric group $\mathcal{S}_n$.*) Let $G = \mathcal{S}_n, n \geqslant 2$, and let c be the cyclic permutation $(1\ 2\ \dots\ n)$. If r, s are distinct elements of $\{1,\dots,n\}$, let $G_{r,s}$ be the subgroup of G generated by c and the transposition $(r\ s)$. Let q be the gcd of n and $|r-s|$.
a) Suppose that $q = 1$. Show that there exists an element of G which normalizes the subgroup generated by c, and conjugates $(r\ s)$ to $(r'\ s')$ with $s' \equiv r' + 1 \pmod{n}$. Use this to show that $G_{r,s} = G$.
b) Suppose that $q > 1$. Show that, if $x, y \in \{1,\dots,n\}$ and $x \equiv y \pmod{q}$, then $\sigma(x) \equiv \sigma(y) \pmod{q}$ for every $\sigma \in G_{r,s}$. Conclude that $G_{r,s}$ is not 2-transitive, and hence is a proper subgroup of G (contrary to what is asserted in Bourbaki [3], §5, exerc.8, as well as in the first edition of Lang [29], I, exerc.38d).
Show that $G_{r,s}$ is isomorphic to the semidirect product (cf. §4.3) of $\mathcal{S}_q$ by a direct product of q copies of $\mathcal{S}_{n/q}$.

22. Let $(N_i)_{i\in I}$ be a finite family of pairwise distinct normal subgroups of a group G. Suppose that the G/N_i are simple and that at most two of them are abelian. Show that the map $G \to \prod_{i\in I} G/N_i$ is surjective.
[Hint: use induction on $|I|$; apply the lemmas of Goursat and Ribet to the image of G in $\prod_{i\in I} G/N_i$.]

23. (*Minimal normal subgroups.*)
a) Let H be a group of finite length which is *characteristically simple*, i.e., is nontrivial and has no characteristic subgroup other than 1 and itself. Show that H is isomorphic

to a finite direct product of simple groups isomorphic to each other.
[Hint: choose a minimal nontrivial normal subgroup N of H. Let X be the set of all the $s(N)$ for $s \in \mathrm{Aut}(H)$; observe that, if $N_1, N_2 \in X$, we have either $N_1 = N_2$ or $N_1 \cap N_2 = 1$. Choose be a finite subset $S = \{N_1, \dots, N_m\}$ of X such that the group G_S generated by the N_i is the direct product of the N_i, and such that S is maximal for that property (note that $m \leqslant \ell(H)$). Show that G_S contains all the subgroups belonging to X (if not, one could enlarge S), hence that it is a characteristic subgroup of G. We thus have $G = G_S = N_1 \times \cdots \times N_m$. Show that N is simple by using the fact that every normal subgroup of N_1 is normal in H.]
b) Let G be a group of finite length and let H be a minimal nontrivial normal subgroup of G. Show that H is isomorphic to a finite direct product of simple groups isomorphic to each other.
[Hint: by a), H has a nontrivial characteristic subgroup H' of the required shape. Since H' is characteristic, it is stable under G-conjugation, hence it is normal in G; the minimality property of H then implies $H' = H$.]

Chapter 2

Sylow theorems

Let p be a prime number and let G be a finite group.

2.1 Definitions

Definition 2.1. *A finite group is called a* ***p-group*** *if its order is a power of* p.

Definition 2.2. *Let* p^n *be the largest power of* p *dividing* $|G|$. *A subgroup* H *of* G *is a* ***p-Sylow subgroup*** *(or a* ***Sylow p-subgroup****) of* G *if* $|H| = p^n$.

Remarks.

1. Let S be a subgroup of G. Then S is a p-Sylow subgroup of G if and only if S is a p-group and $(G : S)$ is prime to p.
2. A conjugate of a p-Sylow subgroup of G is a p-Sylow subgroup of G.

Examples

1) Take $G = \mathbf{Z}/N\mathbf{Z}$, where $N = p^n m$, with m prime to p. By Bézout's theorem we have a canonical isomorphism:

$$\mathbf{Z}/N\mathbf{Z} \simeq \mathbf{Z}/p^n\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z}.$$

The factor $\mathbf{Z}/p^n\mathbf{Z}$ is the unique p-Sylow subgroup of G.

2) Let K be a finite field of characteristic p with $q = p^f$ elements. Let $G = \mathbf{GL}_n(K)$ be the group of $n \times n$ invertible matrices with entries in K. The order of G is the number of K-bases of K^n. Hence:

$$\begin{aligned}|G| &= (q^n - 1)(q^n - q)\cdots(q^n - q^{n-1})\\ &= q^{\frac{n(n-1)}{2}}\prod_{i=1}^{n}(q^i - 1)\\ &= p^{f\frac{n(n-1)}{2}}m,\end{aligned}$$

where $m = \prod_{i=1}^{n} (q^i - 1)$ is prime to p.

Let S be the group of upper triangular matrices with diagonal entries equal to 1. It is a subgroup of G of order $q^{\frac{n(n-1)}{2}} = p^{f\frac{n(n-1)}{2}}$, hence it is a p-Sylow subgroup of G.

2.2 Existence of p-Sylow subgroups

The purpose of this section is to prove the first Sylow theorem:

Theorem 2.1 (Sylow [77]). *Every finite group has a p-Sylow subgroup.*

For the standard proof of this, see exerc.1. We give two other proofs.

2.2.1. First proof.

It relies on the following:

Proposition 2.2. *Let H be a subgroup of G and let S be a p-Sylow subgroup of G. There exists $g \in G$ such that $H \cap gSg^{-1}$ is a p-Sylow subgroup of H.*

Proof. Let $X = G/S$. The group H acts on X by left multiplication. The H-stabilizers of the points of X are of the form $H \cap gSg^{-1}$, with $g \in G$. Since S is a p-Sylow subgroup of G, we have $p \nmid |X|$; hence there is at least one orbit $\mathcal{O} = Hx$ of H whose order is prime to p. Let H_x be the stabilizer of x in H. The group H_x is a p-group of the form $H \cap gSg^{-1}$ (for some g) and $(H : H_x) = |\mathcal{O}|$ is prime to p, which shows that H_x is a p-Sylow subgroup of H.

Corollary 2.3. *If G has a p-Sylow subgroup and if H is a subgroup of G, then H has a p-Sylow subgroup.*

Application : First proof of th.2.1. Let n be the order of G. We embed G into the symmetric group $\mathcal{S}_n$ by making G act on itself by left translations. We embed $\mathcal{S}_n$ in $\mathbf{GL}_n(\mathbf{F}_p)$ as follows: if $\sigma \in \mathcal{S}_n$ and $(e_i)_{1 \leqslant i \leqslant n}$ is a basis of $\mathbf{F}_p^n$, we associate to σ the linear transformation $e_i \mapsto e_{\sigma(i)}$. Thus, G embeds in $\mathbf{GL}_n(\mathbf{F}_p)$. By example 2) in §2.1, the group $\mathbf{GL}_n(\mathbf{F}_p)$ has a p-Sylow subgroup; hence the same is true for G.

2.2.2. Second proof (Miller-Wielandt).

Let $|G| = qm$, where q is a power of p, and m is prime to p. Let X be the set of all the subsets of G of cardinality q. We have $|X| = \binom{qm}{q}$.

Lemma 2.4. $\binom{qm}{q} \equiv m \pmod{p}$.

Proof. Let $R = \mathbf{F}_p[t]$ be the polynomial ring in an indeterminate t over $\mathbf{F}_p$. Since q is a power of p, we have $(1+t)^q = 1+t^q$ in R, hence $(1+t)^{qm} = 1+mt^q+\ldots$ The coefficient of t^q in $(1+t)^{qm}$ is thus m. On the other hand, it is $\binom{qm}{q}$. Hence $\binom{qm}{q}$ and m have the same image in $\mathbf{F}_p$; this proves the lemma.

End of the second proof of th.2.1. The above lemma shows that $|X|$ is prime to p. The group G acts on X by left translations : $A \mapsto gA$, for $g \in G$ and $A \in X$. Since $|X|$ is prime to p, there is at least one orbit $\mathcal{O}$ of G such that $|\mathcal{O}|$ is prime to p. Let A be an element of $\mathcal{O}$ and let H be the set of $g \in G$ such that $gA = A$. We have $|\mathcal{O}| = (G : H)$, hence $(G : H)$ is prime to p, i.e., q divides $|H|$. If $a \in A$, the map $H \to A$ given by $h \mapsto ha$ is injective, hence $|H| \leqslant |A| = q$. Since q divides $|H|$, we have $|H| = q$, and H is a p-Sylow subgroup of G.

Corollary 2.5 (Cauchy). *If p divides the order of G, then G contains an element of order p.*

Proof. Let S be a p-Sylow subgroup of G. Since p divides $|G|$, S is nontrivial. Let x be an element of $S - \{1\}$. The order of x is p^m for some $m \geqslant 1$. Then $x^{p^{m-1}}$ has order p.

2.3 Properties of the p-Sylow subgroups

Theorem 2.6 (Second Sylow theorem, cf. [77])).

(1) *Every p-subgroup of G is contained in a p-Sylow subgroup.*

(2) *The p-Sylow subgroups of G are conjugate to each other.*

(3) *The number of p-Sylow subgroups of G is congruent to 1 modulo p.*

Lemma 2.7. *Let P be a p-group acting on a finite set X. Let X^P be the set of elements of X fixed by P. Then $|X| \equiv |X^P| \pmod p$.*

Indeed, every orbit of P in $X - X^P$ has order divisible by p; hence $|X - X^P|$ is divisible by p.

Proof of parts (1) *and* (2) *of th.2.6.* Let S be a p-Sylow subgroup of G, let P be a p-subgroup of G, and let $X = G/S$. We apply lemma 2.7 to X and P (with P acting on X by left multiplication): since $|X| \not\equiv 0 \pmod p$, we have $|X^P| \not\equiv 0 \pmod p$, hence there exists $x \in X$ fixed by P. The stabilizer of x contains P and is also a conjugate of S. Therefore, P is contained in a conjugate gSg^{-1} of S. This proves part (1). Moreover, if P is a p-Sylow subgroup of G, the inclusion $P \subset gSg^{-1}$ is an equality since the two groups have the same order; this proves part (2).

Proof of part (3). We use the following:

Lemma 2.8. *Let S and S' be two p-Sylow subgroups of G. If S' normalizes S, then $S' = S$.*

Proof of the lemma. The groups S and S' are p-Sylow subgroups of $N_G(S)$. Since S is normal in $N_G(S)$, it is the unique p-Sylow subgroup of $N_G(S)$. Hence $S' = S$.

End of the proof of part (3) *of th.2.6.* Let X be the set of p-Sylow subgroups of G, and let S act on X by conjugation. By lemma 2.8, S is the only element of X fixed by all the elements of S. Lemma 2.7, applied to the action of S on X, shows that $|X| \equiv 1 \pmod{p}$.

Corollary 2.9. *If S is a p-Sylow subgroup of G, then* $\big(G : N_G(S)\big) \equiv 1 \pmod{p}$.

Proof. Part (2) of th.2.6 imply that $(G : N_G(S))$ is the number of the p-Sylow subgroups of G. By part (3), that number is $\equiv 1 \pmod{p}$.

Proposition 2.10. *Let H be a subgroup of G and let P be a p-Sylow subgroup of H. There exists a p-Sylow subgroup S of G such that $P = S \cap H$.*

Proof. This follows from prop.2.2.

Beware that, if S is a p-Sylow subgroup of G, *it is not always true that $S \cap H$ is a p-Sylow subgroup of H*: take for instance for H and S two distinct p-Sylow subgroups. However, this is true when H is normal:

Proposition 2.11. *Let H be a normal subgroup of G and let S be a p-Sylow subgroup of G. Then :*

(1) *$S \cap H$ is a p-Sylow subgroup of H.*

(2) *The image of S in G/H is a p-Sylow subgroup of G/H.*

(3) *Every p-Sylow subgroup of G/H is the image of a p-Sylow subgroup of G.*

(4) *If Q is a p-Sylow subgroup of H, then $HN_G(Q) = G$.*

[Assertion (4) is often referred to as *the Frattini argument.*]

Proof.

(1) By prop.2.10 there exists a p-Sylow S' of G such that $S' \cap H$ is a p-Sylow of H. Since S and S' are conjugate, and H is normal, $S' \cap H$ and $S \cap H$ are G-conjugate, hence have the same order. This implies that $S \cap H$ is a p-Sylow of H.

(2) Let S' be the image of S in G/H. The index of S' in G/H divides $(G : H)$, hence is prime to p. Since S' is a p-group, this implies that S' is a p-Sylow subgroup of G/G.

(3) This follows from (2) since the p-Sylow subgroups of G/H are conjugate.

(4) Let $g \in G$. We have $gQg^{-1} \subset gHg^{-1} = H$. But gQg^{-1} is a p-Sylow subgroup of H; therefore, there exists $h \in H$ such that $gQg^{-1} = hQh^{-1}$. Hence, $h^{-1}g \in N_G(Q)$ and $g \in HN_G(Q)$. This shows that $HN_G(Q) = G$.

Corollary 2.12. *If $f : G \to G'$ is a surjective homomorphism of finite groups, the p-Sylow subgroups of G' are the images of the p-Sylow subgroups of G.*

This is just a reformulation of (2) and (3).

Corollary 2.13. *Let S be a p-Sylow subgroup of G and let H be a subgroup of G containing $N_G(S)$. Then $N_G(H) = H$. In particular $N_G(N_G(S)) = N_G(S)$.*

Proof. Let $K = N_G(H)$. Since H is normal in K, we may apply part (4) of prop.2.11 to K. We obtain $K = HN_K(S)$, hence $K = H$ since $N_K(S) \subset N_G(S) \subset H$.

2.4 Fusion in the normalizer of a p-Sylow subgroup

If S and K are two subgroups of G, with $S \subset K$, two elements (or two subsets) of H are said to **fuse** in K if they are K-conjugate. In this section, we shall be interested in the case where S is a p-Sylow of G, and K is either $N_G(S)$ or G.

Definition and Notation. In what follows, we extend the notion of *normality* in the following way : if X is a subset (not necessarily a subgroup) of G and if H is a subgroup of G, we say that X is *H-normal* if $H \subset N_G(X)$, i.e., if $hXh^{-1} = X$ for every $h \in H$.

Proposition 2.14. *Let S be a p-Sylow subgroup of G, and let $(A_i, B_i)_{i \in I}$ be two families of S-normal subsets of S. Let $g \in G$ be such that $gA_ig^{-1} = B_i$ for every i. Then there exists $n \in N_G(S)$ such that $nA_in^{-1} = B_i$ for every i.*

Proof. Let $N_A = \bigcap_{i \in I} N_G(A_i)$ and $N_B = \bigcap_{i \in I} N_G(B_i)$. We have $gN_Ag^{-1} = N_B$. The hypothesis of S-normality on the A_i and B_i means that $S \subset N_A \cap N_B$, hence $gSg^{-1} \subset N_B$. The groups S and gSg^{-1} are both p-Sylow subgroups of N_B. Hence there exists $z \in N_B$ such that $zSz^{-1} = gSg^{-1}$. The element $n = z^{-1}g$ belongs to $N_G(S)$ and we have $nA_in^{-1} = z^{-1}gA_ig^{-1}z = z^{-1}B_iz = B_i$ for every $i \in I$.

Corollary 2.15. *If two normal subgroups of S are conjugate in G, they are conjugate in $N_G(S)$.*

Theorem 2.16 (Burnside). *Let X and Y be two subsets of the center $Z(S)$ of S. Let $g \in G$ be such that $gXg^{-1} = Y$. Then there exists $n \in N_G(S)$ such that $nxn^{-1} = gxg^{-1}$ for every $x \in X$. In particular, $nXn^{-1} = Y$.*

Proof.
We apply prop.2.14 with $I = X, A_x = \{x\}, B_x = \{gxg^{-1}\}$. Since A_x and B_x are contained in the center of S, they are S-normal. We thus obtain $n \in N_G(S)$ with $nxn^{-1} = gxg^{-1}$ for every $x \in X$.

Corollary 2.17. *Let $x, y \in Z(S)$. If x and y are conjugate in G, they are conjugate in $N_G(S)$.*

Remark. Corollary 2.17 does not extend to arbitrary pairs of elements of S. Here are two examples:

• *Example* 2.4.1. Take $G = S_4$ and $p = 2$. Let S be the subgroup of G made up of the elements $g \in G$ which map the set $\{1, 2\}$ either onto itself or onto its complement $\{3, 4\}$;

it is a 2-Sylow subgroup of G. Let $x = (1\ 2)(3\ 4)$ and $y = (1\ 4)(2\ 3)$. The elements x, y of S are G-conjugate : we have $y = gxg^{-1}$ for $g = (1\ 2\ 3)$; but they are not conjugate in $N_G(S) = S$.

• *Example* 2.4.2. Let p be a prime number. Take $G = \mathrm{GL}_3(\mathbf{F}_p)$, and choose for S its standard p-Sylow subgroup, namely:

$$S = \begin{pmatrix} 1 & \times & \times \\ 0 & 1 & \times \\ 0 & 0 & 1 \end{pmatrix}.$$

Then

$$N_G(S) = \begin{pmatrix} \times & \times & \times \\ 0 & \times & \times \\ 0 & 0 & \times \end{pmatrix}.$$

The elements x and y of S defined by:

$$x = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad y = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix},$$

are conjugate in G but not in $N_G(S)$. Indeed, every $N_G(S)$-conjugate of x is of the form :

$$\begin{pmatrix} 1 & \times & \times \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

2.5 Local conjugation and Alperin's theorem

Let S be a p-Sylow subgroup of G. We have just seen that, for the elements of S, fusion in G is not always the same as fusion in $N_G(S)$. To obtain a general result, we need to replace $N_G(S)$ by $N_G(U)$, where U is a suitable subgroup of S. This leads to the notion of "local conjugation", which is defined as follows:

Two elements $x, y \in S$ are **locally conjugate** if there exists a subgroup U of S containing x and y such that x and y are conjugate in $N_G(U)$.

For instance, the elements x, y of Example 2.4.1 are locally conjugate; the subgroup U that they generate is a normal subgroup of order 4 of $G = \mathcal{S}_4$; hence x, y are conjugate in $N_G(S) = G$.
Example 2.4.2 is different: the elements x, y are not locally conjugate; however, they are both locally conjugate to a third element z, see below. This is typical of what happens in general, as the following theorem shows:

Theorem 2.18 (Alperin). *The equivalence relation on S generated by the relation*

" x and y are locally conjugate "

is the same as the relation " x and y are conjugate in G " .

Equivalently :

Theorem 2.19. *If $x, y \in S$ are conjugate in G, then there exists a sequence of elements $a_0, \ldots, a_n \in S$ such that :*

(1) $a_0 = x$ and $a_n = y$.

(2) a_i is locally conjugate to a_{i+1} for $0 \leqslant i \leqslant n-1$.

Theorem 2.19 follows from the following more general result (in which we write A^g instead of $g^{-1}Ag$):

Theorem 2.20. *Let A be a subset of S and let $g \in G$ such that $A^g \subset S$. Then there exist an integer $n \geqslant 1$, subgroups $U_1, \ldots, U_n$ of S, and elements $g_1, \ldots, g_n$ of G, such that :*

(1) $g = g_1 \cdots g_n$.

(2) $g_i \in N_G(U_i)$ for $1 \leqslant i \leqslant n$.

(3) $A^{g_1 \cdots g_{i-1}} \subset U_i$ for $1 \leqslant i \leqslant n$.

Remarks.

1) For $i = 1$, (3) means that $A \subset U_1$. Note that (2) and (3) imply $A^{g_1 \cdots g_i} \subset U_i$; in particular, we have $A^g \subset U_n$.

2) Theorem 2.19 follows from th.2.20, applied to $A = \{x\}$ and to $g \in G$ such that $g^{-1}xg = y$.

Proof of th.2.20.
Let T be the subgroup of S generated by A. Use induction on the index $(S : T)$. If this index is 1, we have $T = S$ and our assumptions imply that $S^g = S$, i.e., $g \in N_G(S)$. We then take $n = 1$, $g_1 = g$ and $U_1 = S$.

Suppose now $(S : T) > 1$, i.e., $T \neq S$. The group $T_1 = N_S(T)$ is therefore distinct from T, cf. part (1) of th.3.18 (note that the proof of th.3.18 does not use the present theorem, hence there is no logical circle). It is a p-subgroup of $N_G(T)$. Choose a p-Sylow subgroup Σ of $N_G(T)$ containing T_1. By th.2.6, there exists $u \in G$ such that $\Sigma^u \subset S$.

Next, let $V = T^g$. We have $V \subset S$ since $A^g \subset S$. The group Σ^g is a p-Sylow subgroup of $N_G(V) = N_G(T)^g$. Since $N_S(V)$ is a p-subgroup of $N_G(V)$, there exists $w \in N_G(V)$ such that $N_S(V)^w \subset \Sigma^g$.

Set $v = u^{-1}gw^{-1}$. We have $g = uvw$.

We now factor u and v:

(i) We have $T_1^u \subset \Sigma^u \subset S$. Since $(S : T_1) < (S : T)$, the induction hypothesis shows that there exist subgroups $U_1, \ldots, U_m$ of S and elements $u_i \in N_G(U_i)$ with $u = u_1 \cdots u_m$ and $T_1^{u_1 \cdots u_{i-1}} \subset U_i$ for $1 \leqslant i \leqslant m$.

(ii) Set $T_2 = N_S(V)$ and $T_3 = T_2^{v^{-1}} = T_2^{wg^{-1}u}$.
Since $T_2^w \subset \Sigma^g$, we have $T_3 \subset \Sigma^{gg^{-1}u} = \Sigma^u$. The group T_3 is contained in S and $T_3^v = T_2$

is also contained in S. Since $(S : T_3) < (S : T)$, by the induction hypothesis there exist subgroups $V_1, \dots, V_r$ of S and elements $v_j \in N_G(V_j)$ with $v = v_1 \cdots v_r$ and $T_3^{v_1 \cdots v_{j-1}} \subset V_j$ for $1 \leqslant j \leqslant r$. Let us show that the subgroups $U_1, \dots, U_m, V_1, \dots, V_r, V$ of S and the factorization $g = u_1 \cdots u_m v_1 \cdots v_r w$ have the desired properties:

We have

$$u_i \in N_G(U_i),\ v_j \in N_G(V_j),\ w \in N_G(V),$$

and $T^{u_1 \cdots u_{i-1}} \subset U_i$ for $1 \leqslant i \leqslant m$, since $T \subset T_1$.

It remains to check that $T^{u_1 \cdots u_m v_1 \cdots v_{j-1}} \subset V_j \quad$ for $1 \leqslant j \leqslant r$.

We have $T^{gw^{-1}} = V^{w^{-1}} = V \subset N_S(V) = T_2$, hence $T \subset T_2^{wg^{-1}}$ and $T^u \subset T_2^{wg^{-1}u} = T_3$. This implies:

$$T^{u_1 \cdots u_m v_1 \cdots v_{j-1}} = T^{u v_1 \cdots v_{j-1}} \subset T_3^{v_1 \cdots v_{j-1}} \subset V_j,$$

as wanted.

Example. Let us look again at Example 2.4.2. In that case, $G = \mathrm{GL}_3(\mathbf{F}_p)$, and we have two elements x, y of the standard p-Sylow subgroup :

$$x = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad y = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

These elements are conjugate in G: indeed, $y = x^g$, with

$$g = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

Alperin's theorem applies with $n = 2$ and the following choices of g_1 and g_2:

$$g_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \quad g_2 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \text{so that } g = g_1 g_2.$$

We have $x^{g_1} = z$ and $z^{g_2} = y$ with :

$$z = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

The group U_1 is the group generated by x, z; it is normalized by g_1. The group U_2 is generated by z, y; it is normalized by g_2.

2.6 Other Sylow-like theories

This section contains no proofs, and assumes some knowledge of Lie groups and algebraic groups. We give a list of several situations where there are theorems resembling those of Sylow.

In each case, we have a category of groups G and a subcategory P. A P-Sylow subgroup of $G \in \mathsf{G}$ is a subgroup of G which belongs to P and is maximal for that property. The Sylow-like theorems are:

a) *If $H \subset G$, with $H \in \mathsf{P}$ and $G \in \mathsf{G}$, there is a P-Sylow subgroup of G which contains H.*

b) *If $G \in \mathsf{G}$, the P-Sylow subgroups of G are conjugate.*

c) (Burnside's fusion theorem.) *Let S be a P-Sylow subgroup of $G \in \mathsf{G}$. Let A, B be two subsets of $Z(S)$ and let $g \in G$ be such that $gAg^{-1} = B$. Then there exists $n \in N_G(S)$ such that $nan^{-1} = gag^{-1}$ for every $a \in A$.*

d) (Frattini's principle.) *Let $A \subset G$ be an inclusion in the category G. Assume that A is normal in G, and let S be a P-Sylow subgroup of A. Then $G = AN_G(S)$.*

e) (Lifting property of the P-groups) *Let $f : G_1 \to G_2$ be a surjective homomorphism in the category G and let S_2 be a P-Sylow subgroup of G_2. Then there exists a P-Sylow subgroup S_1 of G_1 such that $f(S_1) = S_2$.*

Here are five examples of pairs (G, P) having properties a) to e), with references for proofs of a) and b); as for c) and d), they follow from a) and b) by the same arguments as in standard Sylow theory; property e) is easy for cases 2.6.1 to 2.6.4, and is not difficult for case 2.6.5.

2.6.1. Solvable groups and π-subgroups.
Here G = category of finite solvable groups (cf. §3.2). The subcategory $\mathsf{P} = \mathsf{P}_\pi$ depends on the choice of a set π of prime numbers; a finite group H belongs to P_π if all the prime factors of $|H|$ belong to π. The P_π-Sylow subgroups are called *π-Sylow subgroups.*
Proofs of a) and b) will be given in §5.4.

2.6.2. Compact Lie groups and tori.
Here G = category of compact Lie groups, the morphisms being the continuous homomorphisms; P is the subcategory of tori, i.e., of groups isomorphic to a finite product of copies of $\mathbf{R}/\mathbf{Z}$; the P-Sylow subgroups are the *maximal tori.*
Proofs of a) and b) can be found in many places, e.g., Bourbaki [10], §2.2.

2.6.3. Linear algebraic groups and algebraic tori.
Here G = category of smooth linear algebraic groups over a given algebraically closed field; the morphisms are the so-called regular homomorphisms, see e.g., Borel [2], chap.I. The subcategory P is the category of *algebraic tori*, i.e., of groups isomorphic to a finite product of copies of the multiplicative group $\mathbf{G}_m = \mathrm{GL}_1$.
For a proof of a) and b), see Borel [2], §11.3.

2.6.4. Linear algebraic groups and connected solvable groups.
Here G is the same as in 2.6.3, and P is the subcategory of connected solvable groups.

The P-Sylow subgroups are the *Borel subgroups*.
For a proof of a) and b), see Borel [2], §11.1.

2.6.5. Linear algebraic groups and unipotent groups.
Here G is the same as in 2.6.3, and P is the subcategory of unipotent algebraic groups. Proofs of a) and b) have been given by V.P. Platonov, [70]; the main point is to show that, if a unipotent group U acts on an algebraic linear group G, there exists a Borel subgroup of G which is stable under the action of U ([70], th.3.20).

Let us also mention a property which is **only valid for cases** 2.6.1 **and** 2.6.5:

f) *Let $A \subset G$ be an inclusion in the category* G *, and let S be a* P*-Sylow subgroup of A. Then there exists a* P*-Sylow subgroup T of G, such that $S = A \cap T$.*

This follows from the following fact, which only applies to 2.6.1 and 2.6.5:

g) (A subgroup of a P-group is a P-group.) *Let $A \subset G$ be an inclusion in the category* G*. If $G \in$ P, then $A \in$ P.*

2.7 Exercises

1. (*Proof of the existence of Sylow p-subgroups by reduction to the abelian case.*)
   Let G a finite group, and let p be a prime number. Assume that groups of smaller order, and abelian groups, have p-Sylow subgroups. Let C be the center of G. Suppose that $|G|$ is divisible by p. There are two cases :
   a) The order of C is prime to p. In that case $|G - C|$ is prime to p. Show that there exists a conjugacy class X, contained in $|G - C|$, whose order is prime to p. If $x \in X$, the centralizer of x has index prime to p and is distinct from G, hence has a p-Sylow subgroup; that subgroup is a p-Sylow subgroup of G.
   b) If the order of C is divisible by p, choose a nontrivial p-subgroup C' of C; if S is a p-Sylow subgroup of G/C', the inverse image of S in G is a p-Sylow subgroup of G.

2. (*Sylow*, [77].) Let G be a group acting faithfully and transitively on a set with p elements, p prime. Let H be the subgroup of G generated by the elements of G of order p.
   a) Prove that H is a simple group.
   b) Show that G/H is cyclic of order dividing $p-1$.
   [Hint: let C be a p-Sylow subgroup of G; it is contained in H. Show that the map $N_G(C)/N_H(C) \to G/H$ is surjective.]
   c) Assume $p \geqslant 5$; construct an example where H is nonabelian. Give examples where G/H has order any given divisor of $p-1$.

3. Let G be a finite group, and let p be a prime number.
   a) If H is a subgroup of G, let $O^p(H)$ be the smallest normal subgroup of H of index a power of p (equivalently: $O^p(H)$ is the group generated by the elements of H of order prime to p). Show that, if X is a finite G-set, then $|X^H| \equiv |X^{O^p(H)}| \pmod p$.
   b) Conversely, let H and H' be two subgroups of G such that $|X^H| \equiv |X^{H'}| \pmod p$ for every finite G-set X. Show that $O^p(H)$ and $O^p(H')$ are conjugate in G.
   [Hint: by a), it is enough to prove this when $H = O^p(H)$ and $H' = O^p(H')$. Let $N = N_G(H)$ and let $K = H.S$, where S is a p-Sylow of N; the group K/H is a p-Sylow

of N/H. Let $X = G/K$. The integer $|X^H|$ is equal to $n/|K|$, where n is the number of elements $g \in G$ such that $gHg^{-1} \subset K$, which is the same as $gHg^{-1} = H$ since gHg^{-1} is generated by elements of ordre prime to p. Hence $n = |N|$ and $n/|K|$ is prime to p. Hence $|X^{H'}|$ is prime to p, and this implies that H' fixes a point of X, i.e., is conjugate to a subgroup of K; by the same argument as above, this subgroup is contained in H. Similarly, H is contained in a conjugate of H', hence these two groups are conjugate.]

(*Groups of order pq.*) Let q be a prime number $< p$, and let G be a group of order pq.
a) Show that G has only one p-Sylow subgroup.
[Hint: Use the fact that the number of p-Sylow subgroups is 1 or q, and that it is congruent to 1 mod p.]
b) Suppose that $q \nmid p-1$. Show that G is cyclic.
[Hint: prove first that G has only one q-Sylow subgroup.]
c) Suppose that $q \mid p-1$. Let A be the group of permutations of $\mathbf{F}_p$ of the form $x \mapsto ax+b$, with $a, b \in \mathbf{F}_p$ and $a^q = 1$. Show that $|A| = pq$, that $Z(A) = 1$ and that $\mathrm{Out}(A)$ is cyclic of order $\frac{p-1}{q}$.
Show that a group of order pq is either cyclic or isomorphic to A.

4. (*Order of a p-Sylow subgroup of $\mathcal{S}_n$.*) Let n be an integer > 0. It may be written in a unique way as:

$$n = n_0 + n_1 p + n_2 p^2 + \cdots,$$

with $0 \leqslant n_i \leqslant p-1$ and $n_i = 0$ for i large enough (*base p expansion of n*). Show that the highest power of p which divides $n!$ is $p^{s(n)}$, where

$$s(n) = \sum_m n_m \frac{p^m - 1}{p-1} = \frac{n - n_0 - n_1 - n_2 - \cdots}{p-1}.$$

[Hint: show first that $s(n) = [n/p] + [n/p^2] + \cdots$, where $[x]$ is the *integral part* of x, i.e., the largest integer $\leqslant x$.]

5. (*Binomial coefficients mod p.*) Let n, m be two positive integers, written in base p as in exerc.4:

$n = n_0 + n_1 p + n_2 p^2 + \cdots$, and $m = m_0 + m_1 p + m_2 p^2 + \cdots$ with $0 \leqslant n_i, m_i \leqslant p-1$.

Show that $\binom{n}{m} \equiv \prod \binom{n_i}{m_i} \pmod p$.

[Hint: Use the method of proof of lemma 2.4, i.e., compute $(1+t)^n$ in $\mathbf{F}_p[t]$.]

6. (*Structure of a p-Sylow subgroup of $\mathcal{S}_n$.*)
a) Write n as in exerc.4: $n = n_0 + n_1 p + n_2 p^2 + \ldots$. Show that $\mathcal{S}_n$ has a subgroup Σ_n isomorphic to $\prod_m (\mathcal{S}_{p^m} \times \cdots \times \mathcal{S}_{p^m})$, where each $\mathcal{S}_{p^m}$ is repeated n_m times. Show that the index of Σ_n in $\mathcal{S}_n$ is prime to p; hence a p-Sylow subgroup of $\mathcal{S}_n$ is isomorphic to a product $\prod_m (H_m \times \cdots \times H_m)$, where H_m is a p-Sylow subgroup of $\mathcal{S}_{p^m}$.
b) Let m be an integer $\geqslant 0$, and let $X_m = (\mathbf{F}_p)^m$, so that $\mathcal{S}_{X_m} \simeq \mathcal{S}_{p^m}$. Let H_m be the subgroup of $\mathcal{S}_{X_m}$ made up of the permutations:

$$\begin{aligned} x_1 &\mapsto x_1 + a_1, \\ x_2 &\mapsto x_2 + a_2(x_1), \\ &\cdots \\ x_m &\mapsto x_n + a_m(x_1, \ldots, x_{n-1}), \end{aligned}$$

where $a_1 \in \mathbf{F}_p$ and a_i is a map of X_{i-1} into $\mathbf{F}_p$ if $i \geqslant 2$.
Show that H_m is a p-Sylow of $\mathcal{S}_{X_m}$, hence is isomorphic to a p-Sylow of $\mathcal{S}_{p^m}$.

7. (*Uniqueness of a simple group of order* 60.) Let G be a simple group of order 60.
a) Show that the number of the 5-Sylow subgroups of G is 6.
[Hint: use the fact that this number is > 1, divides 60, and is $\equiv 1 \pmod 5$).]
b) The conjugaison action of G on its 5-Sylow subgroups gives an embedding $G \subset \mathcal{A}_6$. The set $\mathcal{A}_6/G$ has 6 elements. The action of G on that set fixes one element; show that its action on the other five gives an embedding $G \to \mathcal{A}_5$ which is an isomorphism. Hence $G \simeq \mathcal{A}_5$.
[For a different proof, using the 2-Sylow subgroups, see chap.7, proof of th.7.22.]

8. (*Outer automorphisms of* $\mathcal{S}_6$.)
Let $I = \{1, \ldots, 6\}$ and J = set of 5-Sylow subgroups of $\mathcal{S}_6$.
a) The group $\mathcal{S}_6$ acts transitively on both I and J, which have 6 elements. Show that these actions are not isomorphic.
[Hint: use the fact that the subgroup $\mathcal{S}_5$ of $\mathcal{S}_6$ fixes a point of I but does not fix a point of J.]
b) Deduce from a) that $\mathcal{S}_6$ has an automorphism which is not inner[1], and which permutes the two classes of elements of order 3 of $\mathcal{S}_6$, as well as the two classes of elements of order 2 of $\mathcal{S}_6 - \mathcal{A}_6$.
c) Show that $\mathcal{S}_6$ contains two conjugacy classes of subgroups isomorphic to $\mathcal{S}_5$.

9. Let S be a p-Sylow subgroup of G. Show that the orbits of $N_G(S)$, acting on the set of all S-normal subsets of S, have order prime to p.

10. (*Construction of subgroups of index 2.*) Let S be a 2-Sylow subgroup of a finite group G and let H be a subgroup of S. Let $\varepsilon_H : G \to \{\pm 1\}$ be the homomorphism defined by $\varepsilon_H(g)$ = signature of the permutation $x \mapsto gx$ of G/H.
Let C be a nontrivial cyclic subgroup of S. Assume that $|C| \cdot |H| = |S|$ and that $C \cap gHg^{-1} = 1$ for every $g \in G$.
a) Show that C acts freely on G/H, and that the number of its orbits is odd.
b) Use a) to show that $\varepsilon_H(C) = \{1, -1\}$; hence the kernel of ε_H is a subgroup of G of index 2 which does not contain C.

11. (*Construction of normal 2-complements - the abelian case.*) Let S be a 2-Sylow subgroup of a finite group G. Assume that S is abelian and that there is *no fusion* among the elements of S of order 2, i.e., that, if two such elements are G-conjugate, they are equal. Note that this hypothesis is satisfied if S is cyclic.
Let N be the set of elements of G of odd order. Show that N is a normal subgroup of G, and that the map $S \to G/N$ is an isomorphism (i.e., N is a **normal complement**[2] of S in G).
[Hint: Use induction on $|S|$. If $|S| > 1$, write S as $C \times H$, with C nontrivial cyclic (this

[1] The group $\mathrm{Out}(\mathcal{S}_6)$ has order 2 and $\mathrm{Out}(\mathcal{S}_n) = 1$ for $n \neq 6$, cf. Huppert [25], Kap.II, Satz 5.5, or Bourbaki [3], chap.I, §5, exerc.23.

[2] If A and B are two subgroups of a group G, one says that A is a **complement** of B in G if $AB = G$ and $A \cap B = 1$. When B is a p-Sylow subgroup of G, A is called a **p-complement**, cf. §5.6. A **normal complement** is a complement which is normal in G; in that case G is the semidirect product (see §4.3) of the two subgroups.

is possible, see th.3.22) and use exerc.10 to show that G has a subgroup G' of index 2; show that G' contains N and that all the elements of order 2 of G' are G'-conjugate. Apply the induction hypothesis to G'.]

12. Let G be a finite simple group. Show that, if $|G| \equiv 2 \pmod 4$, then $|G| = 2$.
[Hint: use exerc.11.]

13. (*Construction of normal 2-complements - the dihedral case.*)
Let S be a 2-Sylow subgroup of a finite group G. Assume that S is dihedral [3] of order $\geqslant 4$ and that, if two elements of order 2 of S are G-conjugate, then they are S-conjugate (*no fusion*). Show that the elements of odd order of G make up a normal complement of S.
[Hint: let H be a cyclic subgroup of index 2 of S (there is only one such if $|S| \geqslant 8$). Exercise 10, applied to H and to $\{1, g\}$, shows that $\varepsilon_H(g) = -1$ for every $g \in S - H$. Hence the kernel G' of ε_H contains H and H is a 2-Sylow of G'. Conclude by applying exerc.11 to G'.]

14. (*Fusion patterns when $S = \mathcal{D}_4$.*) Let S be the dihedral group $\mathcal{D}_4$ of order 8, and let G be a finite group containing S as a 2-Sylow subgroup.
a) Show that S has 5 elements of order 2, which form 3 conjugacy classes: a central element c, two conjugate elements s_1, s_1' with $s_1' = s_1c$, and two conjugate elements s_2, s_2' with $s_2' = s_2c$.
b) Show that it is possible to choose G such that there is *maximal fusion*, namely, the elements $\{c, , s_1, s_1', s_2, s_2'\}$ are G-conjugate.
[Hint: take $G = \mathcal{A}_6$.]
In that case, G has only one conjugacy class of elements of order 2; show that it does not have any subgroup of index 2.
[Hint: show first that S is contained in the derived group $D(G)$, cf. §3.1.]
c) Show that it is possible that c and s_1 are G-conjugate, without being G-conjugate to s_2 (*small fusion*).
[Hint: take $G = \mathcal{S}_4$.]
In that case, G has 2 conjugacy classes of elements of order 2; it has a subgroup of index 2: this follows from exerc.10, applied to $H = \{1, c, s_1, cs_1\}$ and $C = \{1, s_2\}$.
d) Show that it is possible that there is *no fusion* : G has 3 conjugacy classes of elements of order 2. In that case, S has a normal complement in G, cf. exerc.13.
e) Show that it is impossible that s_1 and s_2 are G-conjugate without being G-conjugate to c.
[Hint: Let G be such a group. Apply th.2.19 to s_1, s_2. One obtains a sequence of elements $a_1, \ldots, a_n$ of S with $a_1 = s_1$, $a_n = s_2$, and a_i locally conjugate to a_{i+1} for $0 \leqslant i \leqslant n-1$. The a_i are of order 2, and, by hypothesis, they are not equal to c; hence they are S-conjugate to either s_1 or s_2. There is a least one i such that a_i and a_{i+1} are not in the same S-class. For such an i, the only subgroup of S containing both of them is S itself. Hence s_1 and s_2 are $N_G(S)$-conjugate. But that is impossible, since the orbits of $N_G(S)$ on the S-conjugation classes have odd order, cf. exerc.9.]
f) The group S has two elementary subgroups of type $(2, 2)$, namely $\{1, s_1, s_1', c\}$ and

[3] Recall that the **dihedral** group $\mathcal{D}_m$ of order $2m$ is generated by elements c and s of order respectively m and 2 with $scs = c^{-1}$. When $m \geqslant 3$, it is the symmetry group of a regular m-gon in the euclidean plane; when $m = 2$, it is an elementary abelian group of order 4.

$\{1, s_2, s'_2, c\}$. Show that these subgroups are not G-conjugate.
[Hint: if they were, by cor.2.15, they would be $N_G(S)$-conjugate. Use the same argument as in e) to show that this is impossible.]

15. (*Fusion patterns when S is the quaternion group of order* 8.)
Let $S = \{\pm 1, \pm i, \pm j, \pm k\}$ be the quaternion group of order 8.
a) Show that $\mathrm{Aut}(S) \simeq \mathcal{S}_4$ and $\mathrm{Out}(S) \simeq \mathcal{S}_3$.
[Hint: use the action of $\mathrm{Aut}(S)$ on the three subgroups of S of order 4.]
b) Let G be a finite group containing S as a 2-Sylow subgroup. The action of $N_G(S)$ on S defines a homomorphism $\varphi : N_G(S) \to \mathrm{Aut}(S) \to \mathrm{Out}(S)$. The image of φ has order 1 or 3. Check that the image of φ has order 3 (*total fusion*) when $G = \mathrm{SL}_2(\mathbf{F}_3)$.
[This holds more generally when $G = \mathrm{SL}_2(\mathbf{F}_q)$ with $q \equiv \pm 3 \pmod 8$.]
c) Assume that φ is trivial. Then:
c_1) Show that two distinct subgroups of order 4 of S are not G-conjugate (*no fusion*).
[Hint: use prop.2.14.]
c_2) Let C be a subgroup of order 4 of S, and let $\varepsilon_C : G \to \{1, -1\}$ be the corresponding homomorphism, cf. exerc.10. Let c be the element of order 2 of S. Let $X = G/C$, let Y be the subset of X fixed by c and let $Z = X - Y$. Show that G acts freely on Z, hence $|Z| \equiv 0 \pmod 8$, which implies $|Y| \equiv 2 \pmod 4$.
c_3) Let C' be a subgroup of order 4 of S, with $C' \neq C$. Show that C' does not fix any point of X, and that its orbits have order 2 on Y and order 4 on Z; conclude that the total number of its orbits is odd, hence that ε_C is nontrivial on C'. Show that ε_C is trivial on C [use the fact that a generator of C is the product of two elements of order 4 which do not belong to C].
c_4) Let G' be the kernel of ε_C. Show that C is a 2-Sylow subgroup of G'. Conclude that C has a normal complement in G'; hence S has a normal complement in G.

16. (*Index of the center.*)
a) Let G be a group. Show that $(G : Z(G)) \neq 15$.
[Hint: use exerc.3, together with exerc.1 of chap.1.]
b) There are nineteen integers (2,3,...,45,47) below 50 which are $\neq (G : Z(G))$ for every group G. Find them.
[Hint: all the numbers on that list are prime numbers, except four of them: three of these are similar to 15, and the fourth one (45) requires a longer proof.]
For each of the others (1,4,...,48,49), construct a finite group G such that $(G : Z(G))$ is equal to that number.
[Example: if n is even $\geqslant 4$, take for G a dihedral group of order $2n$.]

Chapter 3

Solvable groups and nilpotent groups

3.1 Commutators and abelianization

Let G be a group and let $x, y \in G$. The element $x^{-1}y^{-1}xy$ is called the **commutator** [1] of x and y, and is denoted by (x, y). We have

(1.1) $\quad xy = yx(x, y).$

Let us collect a few identities, cf. Bourbaki [3], §6.2. Define first

(1.2) $\quad x^y = y^{-1}xy = \mathrm{int}_{y^{-1}}(x) = x(x, y).$

Then:

(1.3) $\quad (x, yz) = (x, z).(x, y)^z = (x, z).(z, (y, x)).(x, y), \quad$ for every $x, y, z \in G$:

(1.4) $\quad (x, yz).(z, xy).(y, zx) = 1,$

(1.5) $\quad (x^y, (y, z)).(y^z, (z, x)).(z^x, (x, y)) = 1.$

These identities are proved by explicit computation; for instance, when *Hall's identity* (1.5) is written down explicitly, it has 42 terms which cancel each other. Note also the analogy between (1.5) and the Jacobi identity $[x, [y, z]] + [y, [z, x]] + [z, [x, y]] = 0$ in the theory of Lie algebras; for a precise connection between the two, see §3.4.

Let A and B be subgroups of G. We write (A, B) for the group generated by the commutators (x, y) with $x \in A$ and $y \in B$.

The group (G, G) is called the **commutator subgroup**, or the **derived group**, of G, and is denoted by $D(G)$. It is a characteristic subgroup of G. We have:

Proposition 3.1. *Let H be a subgroup of G. Then the following properties are equivalent :*

(1) *H contains $D(G)$.*

(2) *H is normal and G/H is abelian.*

[1] We follow here Bourbaki's convention, cf. [3], §6.2; a more usual one is to define the commutator as $xyx^{-1}y^{-1}$; this does not make much difference in the formulas; see exerc.4.

Thus, $G/D(G)$ is the maximal abelian quotient of G. It is called the **abelianization** of G and it is denoted by G^{ab}. Every homomorphism of G into an abelian group can be factored through $G \to G^{\mathrm{ab}}$.

Examples. 1. Let $G = \mathrm{GL}_n(K)$, where K is a field, and $n \geqslant 1$. Then $D(G) = \mathrm{SL}_n(K)$ and $\mathrm{GL}_n(K)^{\mathrm{ab}} \simeq K^\times$, except when $n = 2$ and $|K| \leqslant 3$, in which case $\mathrm{GL}_2(K)^{\mathrm{ab}} \simeq K$.

2. If $n \geqslant 2$, then $\mathcal{S}_n^{\mathrm{ab}} \simeq \{\pm 1\}$.

3.2 Solvable groups

The functor $G \rightsquigarrow D(G)$ can be iterated; we thus obtain a sequence $D^n G$ of subgroups of G:

$$D^0 G = G, \quad D^1 G = D(G), \quad D^n G = (D^{n-1}G, D^{n-1}G) = D(D^{n-1}G) \quad \text{for } n \geqslant 1.$$

We have $G \supset D^1 G \supset D^2 G \supset \cdots$. The intersection of the $D^n G$ is denoted by $D^\infty G$.

Definition 3.1. *A group G is* ***solvable*** *(**soluble** in British English) if there exists an integer $n \geqslant 0$ such that $D^n G = 1$. The smallest integer n such that $D^n G = 1$ is called the* ***derived length*** *or the* ***solvability class*** *of G and is denoted by $d\ell(G)$.*

Therefore, $d\ell(G) = 0$ is equivalent to $G = 1$ and $d\ell(G) \leqslant 1$ means that G is abelian.

Proposition 3.2. *Let G be a group and let n be an integer $\geqslant 1$. The following properties are equivalent :*

(1) *G is solvable with $d\ell(G) \leqslant n$.*

(2) *There exists a sequence $G = G_0 \supset G_1 \supset \cdots \supset G_n = 1$ of characteristic subgroups of G such that G_i/G_{i+1} is abelian, for $0 \leqslant i \leqslant n-1$.*

(2′) *There exists a sequence $G = G_0 \supset G_1 \supset \cdots \supset G_n = 1$ of subgroups of G such that G_i is normal in G_{i-1} and G_{i-1}/G_i is abelian, for $1 \leqslant i \leqslant n$.*

(3) *There exists a characteristic abelian subgroup A of G such that G/A is solvable with $d\ell(G/A) \leqslant n-1$.*

Proof. Use induction on n, the case $n = 1$ being trivial.

(1) $\Longrightarrow$ (2): For $i \geqslant 0$, set $G_i = D^i G$.

(2) $\Longrightarrow$ (2′): This is clear.

(2′) $\Longrightarrow$ (1): By induction on k and prop.3.1, we have $D^k G \subset G_k$ for $k \geqslant 0$, hence $D^n G = 1$. Note that this already shows that (1), (2) and (2′) are equivalent.

(1) $\Longrightarrow$ (3): Take $A = D^{n-1}G$.

(3) $\Longrightarrow$ (2): By the induction assumption, applied to G/A, there exists a sequence of normal subgroups $A_0, \ldots, A_{n-1}$ of G with $A_0 = G \supset A_1 \supset \cdots \supset A_{n-1} = A$ such that

$$G/A \supset A_1/A \supset \cdots \supset A_{n-1}/A = 1$$

satisfies condition (2).

Corollary 3.3. *Assume that G is solvable, finite and nontrivial.*
(i) Then there exists a prime number p and a characteristic nontrivial p-subgroup N of G which is elementary abelian.
(ii) (Jordan) *Let H be a maximal proper subgroup of G. Then $(G : H)$ is a power of a prime number.*

[A finite abelian p-group is called **elementary** if every non-identity element has order p, i.e., if it is a direct product of cyclic groups of order p.]

Proof of (i). If $d\ell(G) = 1$, G is abelian; if p is a prime divisor of $|G|$, choose for N the set of elements $x \in G$ such that $x^p = 1$. If $d\ell(G) > 1$, choose an abelian subgroup A of G having property (3) above, and take for N the set of $a \in A$ with $a^p = 1$, where p is a prime divisor of $|A|$.
Proof of (ii). Use induction on $|G|$. Let N be as in (*i*). If $N \subset H$, then (ii) follows by the induction hypothesis applied to G/N and H/N. If $N \not\subset H$, then $G = HN$ (because H is maximal), and $G/H \simeq N/N \cap H$; since N is a p-group, $(N : N \cap H)$ is a power of p.

Remark. Every subgroup, and every quotient group, of a solvable group with derived length $\leqslant n$ is solvable with derived length $\leqslant n$.

Proposition 3.4. *Let N be a normal subgroup of G. If N and G/N are solvable, so is G, and $d\ell(G) \leqslant d\ell(N) + d\ell(G/N)$.*

Proof. Let $i = d\ell(N)$ and $j = d\ell(G/N)$. We have $D^j(G) \subset N$, and $D^i(N) = 1$, hence $D^{i+j}(G) = D^i(D^jG) = 1$. The proposition follows.

Proposition 3.5. *Let G be a finite group and let $G = G_0 \supset G_1 \supset \cdots \supset G_n = 1$ be a Jordan-Hölder filtration of G. The group G is solvable if and only if G_i/G_{i+1} is a cyclic group of prime order, for $0 \leqslant i \leqslant n-1$.*

Proof. Note that G_i/G_{i+1} is both simple and solvable, hence its derived group is trivial, which implies that it is cyclic of prime order.

Examples.

1. The group $\mathcal{S}_n$ is solvable if and only if $n \leqslant 4$.

2. A simple nonabelian group is not solvable.

3. Let V be a vector space of dimension n over a field K and let

$$V = V_0 \supset V_1 \supset \cdots \supset V_n = 0$$

be a **complete flag** (i.e., a decreasing sequence of subspaces of the vector space V such that $\mathrm{codim}(V_i) = i$ for each i). We set

$$G = \{s \in \mathbf{GL}(V) \mid sV_i = V_i,\ 0 \leqslant i \leqslant n\}.$$

(If we choose a basis of V adapted to the flag, G becomes the group of invertible upper triangular matrices.)

Define a decreasing sequence of subgroups $(B_i)_{0 \leqslant i \leqslant n}$ of G by

$$B_i = \{g \in G \mid (g-1)V_j \subset V_{i+j},\ 0 \leqslant j \leqslant n-i\}.$$

In particular, $B_0 = G$ and $B_n = 1$.

We have $(B_j, B_k) \subset B_{j+k}$ *if* $0 \leqslant j+k \leqslant n$.

Indeed, let $s \in B_j$, $t \in B_k$, and $x \in V_i$. There exists $v \in V_{i+k}$ and $w \in V_{i+j}$ such that $tx = x + v$ and $sx = x + w$. Then :

$$stx = s(x+v) = x + w + v + t', \quad \text{with } t' \in V_{i+j+k}.$$

Similarly :

$$tsx = t(x+w) = x + v + w + t'', \quad \text{with } t'' \in V_{i+j+k}.$$

Therefore, $stx \equiv tsx \pmod{V_{i+j+k}}$, i.e., $s^{-1}t^{-1}stx \equiv x \pmod{V_{i+j+k}}$, giving the desired result. In particular, we have

- $(B_0, B_i) \subset B_i$ for $0 \leqslant i \leqslant n$, hence B_i is normal in $B_0 = G$.
- $(B_i, B_i) = D(B_i) \subset B_{2i} \subset B_{i+1}$ for $1 \leqslant i \leqslant n$, hence the quotients B_i/B_{i+1} are abelian for $1 \leqslant i \leqslant n-1$.
- The quotient $B_0/B_1 = G/B_1$ is isomorphic to the group of diagonal matrices, which is abelian.

The sequence $B_0 = G \supset B_1 \supset \cdots \supset B_n = 1$ satisfies condition (2) of prop.3.2, and thus G is solvable.

[For a generalization, see exerc.8.]

4. We shall see later (Burnside's theorem, cf. th.5.4 and th.8.62) that every group of order $p^a q^b$, where p and q are prime numbers, is solvable.

5. Every group *of odd order* is solvable (Feit-Thompson's theorem, cf. [55]) . Equivalently: the order of a nonabelian finite simple group is divisible by 2 (it is even divisible by 4, see chap.2, exerc.12).

6. Solvable groups in Galois theory: Let K be a field of characteristic 0 and let $\overline{K}$ be an algebraic closure of K. Let K_{rad} be the smallest subfield of $\overline{K}$ containing K such that for all $x \in K_{rad}$ and for all integer $n \geqslant 1$, there exists an n-th root of x which belongs to K_{rad}. One can show (see e.g. Lang [29], VI.7.2) that a finite Galois extension of K is contained in K_{rad} if and only if its Galois group is solvable (i.e., an equation is *solvable by radicals* if and only if its Galois group is solvable). This explains the use in group theory of the word "solvable".

3.3 Descending central series and nilpotent groups

Let G be a group. The **descending central series** of G is the sequence of subgroups $(C^nG)_{n\geqslant 1}$ of G defined inductively by:

$$C^1G = G \quad \text{and} \quad C^{n+1}G = (G, C^nG) \quad \text{for } n \geqslant 1.$$

For all $n \geqslant 1$, C^nG is a characteristic subgroup of G. The intersection of the C^nG is denoted by $C^\infty G$.

Proposition 3.6. *We have $(C^iG, C^jG) \subset C^{i+j}G$ for all $i \geqslant 1$ and $j \geqslant 1$.*

Proof. Use induction on i. The proposition is clear when $i = 1$ and $j \geqslant 1$. Fix $j \geqslant 1$. We have $(C^iG, C^jG) = \big((G, C^{i-1}G), C^jG\big)$. But $\big((C^{i-1}G, C^jG), G\big)$ is contained in $(C^{i+j-1}G, G)$ by the induction hypothesis; therefore, $\big((C^{i-1}G, C^jG), G\big) \subset C^{i+j}G$. Similarly, $\big((C^jG, G), C^{i-1}G\big) \subset C^{i+j}G$. The following lemma, applied to the groups $X = G$, $Y = C^{i-1}G$, $Z = C^jG$ and $H = C^{i+j}G$, shows that $(C^iG, C^jG) \subset C^{i+j}G$.

Lemma 3.7. *If X, Y and Z are normal subgroups of G and if H is a subgroup of G containing $\big((Y,Z),X\big)$ and $\big((Z,X),Y\big)$, then H contains $\big((X,Y),Z\big)$.*

Proof. After dividing G by the subgroup generated by $\big((Y,Z),X\big)$ and $\big((Z,X),Y\big)$, we may assume that $\big((Y,Z),X\big) = 1 = \big((Z,X),Y\big)$, and we have to prove that $\big((X,Y),Z\big) = 1$. This means showing that every $\zeta \in Z$ commutes with every commutator (x,y), with $x \in X$ and $y \in Y$. Let $z = x\zeta x^{-1}$; we have $z^x = \zeta$. If we apply Hall's identity (1.5) to x, y, z, the first two terms are equal to 1 and the third one is $(\zeta, (x,y))$. Hence $(\zeta, (x,y)) = 1$, as wanted.

Definition 3.2. *A group G is called **nilpotent** if there exists an integer $n \geqslant 0$ such that $C^{n+1}G = 1$. The **nilpotency class** of G is the smallest such integer n.*

For instance:

- The group G is trivial (resp. abelian) if and only if its nilpotency class is 0 (resp. is $\leqslant 1$).

- A finite product of nilpotent groups is nilpotent and the nilpotency class of the product is the maximum of the nilpotency classes of the groups.

- A subgroup (resp. a quotient group) of a nilpotent group is nilpotent.

Proposition 3.8. *A nilpotent group is solvable.*

Proof. Indeed, for every $n \geqslant 0$, we have $D^nG \subset C^{2^n}G$; hence $D^nG = 1$ when n is large enough.

The converse is false: the group $\mathcal{S}_3$ is solvable of derived length 2; its descending central series is such that $C^i\mathcal{S}_3 = \mathcal{A}_3$, for $i \geqslant 2$; hence it is not nilpotent.

A group G is called a **central extension** of a group Γ by an abelian group A if there exists an exact sequence $1 \to A \to G \to \Gamma \to 1$ with A contained in the center of G.

Proposition 3.9. *A group G is nilpotent of nilpotency class $\leqslant n$, with $n > 0$, if and only if G is a central extension of a nilpotent group Γ of nilpotency class $\leqslant n-1$.*

Proof. If G has nilpotency class $\leqslant n$, then $C^{n+1}G = 1$, i.e., C^nG is contained in the center of G. Define $\Gamma = G/C^nG$. We have $C^n\Gamma = 1$; therefore, Γ is nilpotent of nilpotency class $\leqslant n-1$.
Conversely, if such an exact sequence exists with $C^n\Gamma = 1$, then $C^nG \subset A$; therefore, C^nG is contained in the center of G, and $C^{n+1}G = 1$.

Corollary 3.10. *If G is nilpotent and nontrivial, then $Z(G)$ is nontrivial.*

More precisely:

Corollary 3.11. *A group G is nilpotent of nilpotency class $n > 0$ if and only if $G/Z(G)$ is nilpotent of nilpotency class $n-1$.*

Note that this gives an inductive definition both of nilpotency and of the nilpotency class.

Corollary 3.12. *Let G be a nilpotent group and let H be a proper subgroup of G. Then :*
a) $N_G(H) \neq H$.
b) The following properties are equivalent :

(i) H is maximal among the proper subgroups of G.

(ii) The index of H in G is a prime number.

(iii) H is normal and G/H is cyclic of prime order.

Proof of a). Use induction on the nilpotency class n of G. If $n = 1$, then G is abelian and $N_G(H) = G$, hence $N_G(H) \neq H$. If $n \geqslant 2$, let $A = Z(G)$. The group G/A is nilpotent of nilpotency class $n-1$. We have $N_G(H) \supset A$. If $H \not\supset A$, then $N_G(H) \neq H$. If $H \supset A$, then H/A is a subgroup of G/A and the induction hypothesis shows that $H/A \neq N_{G/A}(H/A)$. Since $N_G(H)/A = N_{G/A}(H/A)$, this shows that $N_G(H) \neq H$.

Proof of b). The implications $(iii) \Longrightarrow (ii) \Longrightarrow (i)$ are clear. Conversely, if H is maximal, then *a)* shows that it is normal in G. The group G/H has no proper subgroup distinct from 1. This implies that it is cyclic of prime order. Hence $(i) \Longrightarrow (iii)$.

3.4 Nilpotent groups and Lie algebras

3.4.1. Central filtrations.

Let $G = G_1 \supset G_2 \supset \cdots \supset G_n \supset \cdots$ be a decreasing sequence of subgroups of a group G such that $G_n = 1$ for large enough n. Such a sequence is called a **central filtration** if $(G_i, G_j) \subset G_{i+j}$ for every i, j, cf. Bourbaki [8], chap.II, § 4.4. [Note that, here, the filtration starts with G_1 and not with G_0.] We have:

Proposition 3.13. *Let G be a group. The following properties are equivalent :*
(1) G is nilpotent.
(2) G has a central filtration.

Proof. We have (1) $\Longrightarrow$ (2) by taking $G_i = C^iG$. Conversely, if (G_i) is a central filtration of G, we have $C^iG \subset G_i$ for all i, hence $C^iG = 1$ for large enough i.

Example. Let V be a vector space of dimension n over a field K and let

$$V = V_0 \supset V_1 \supset \cdots \supset V_n = 0$$

be a complete flag of V. Take the example given in §3.2 and let

$$B_i = \{g \in \mathbf{GL}(V) \mid (g-1)V_j \subset V_{i+j} \text{ for all } j\}.$$

Then B_1 is nilpotent; indeed, $(B_i)_{i \geqslant 1}$ is a central filtration of B_1.

3.4.2. The Lie algebra associated to a central filtration.

Let $G = G_1 \supset G_2 \supset \cdots \supset G_n \supset \cdots$ be a central filtration of G, and let

$$\operatorname{gr}(G) = \bigoplus_i \operatorname{gr}_i(G) \quad \text{where} \quad \operatorname{gr}_i(G) = G_i/G_{i+1},$$

be the corresponding graded group, which we write additively.

If $\xi \in \operatorname{gr}_i(G)$ and $\eta \in \operatorname{gr}_j(G)$, define their *bracket* $[\xi, \eta] \in \operatorname{gr}_{i+j}(G)$ as the class of the commutator (x, y) mod G_{i+j+1} , where x (resp. y) is a representative in G_i (resp. G_j) of ξ (resp. η); it is independent of the choice of representatives, as one sees by applying formulas (1.3) and (1.4). We thus obtain a *Lie algebra structure* on $\operatorname{gr}(G)$: the bracket is bilinear, we have $[\xi, \xi] = 0$, and (1.5) shows that :

$$[\xi_1, [\xi_2, \xi_3]] + [\xi_2, [\xi_3, \xi_1]] + [\xi_3, [\xi_1, \xi_2]] = 0 \qquad \text{(Jacobi identity)}.$$

This applies in particular when G is nilpotent and $G_i = C^i(G)$. In that case, the Lie algebra $\operatorname{gr}(G)$ has the following property :

(*) *If $n \geqslant 2$, then $\operatorname{gr}_n(G)$ is generated by brackets of type $[\xi, \eta]$, with $\xi \in \operatorname{gr}_1(G)$ and $\eta \in \operatorname{gr}_{n-1}(G)$.*

This follows from the equality $C^nG = (G, C^{n-1}G)$.

One thus obtains a "linearizing" functor:

$$\textbf{Groups} \rightsquigarrow \textbf{Lie algebras}.$$

This is often useful, if only because addition is easier to handle than multiplication. Here is a simple example:

Theorem 3.14. *Let G be a nilpotent group.*
(a) Let $\varphi : H \to G$ be a homomorphism of a group H into G. If $H \xrightarrow{\varphi} G \to G^{\mathrm{ab}}$ is surjective, then φ is surjective.
(b) Let $\psi : G \to H$ be a homomorphism of G into a group H. If $Z(G) \to G \xrightarrow{\psi} H$ is injective, then ψ is injective.

Proof of (a). Define $\mathrm{gr}_n(G) = C^nG/C^{n+1}G$ and $\mathrm{gr}_n(H) = C^nH/C^{n+1}H$, as above. The map $\varphi : H \to G$ defines for every n a homomorphism $\varphi_n : C^nH \to C^nG$, hence also a homomorphism $\varepsilon_n : \mathrm{gr}_n(H) \to \mathrm{gr}_n(G)$. Note that $\mathrm{gr}_1(G) = G^{\mathrm{ab}}$, so that, by assumption, ε_1 is surjective. Using property (*) above, this shows, by induction on n, that ε_n is surjective for every n. Hence the $\varphi_n : C^nH \to C^nG$ are surjective: indeed, this is true for n large enough (since $C^nG = 1$), and, if it is true for $n+1$, it is true for n because ε_n is surjective. For $n = 1$, this gives the surjectivity of φ.

Proof of (b). Assertion (b) can be restated as:

Lemma 3.15. *Let N be a normal subgroup of a nilpotent group G. Then $N \cap Z(G) \neq 1$ if $N \neq 1$.*

Proof of lemma 3.15. Let n be the largest integer such that the group $N_n = N \cap C^nG$ is nontrivial. The group (G, N_n) is contained in $N \cap C^{n+1}G$, hence is trivial. This shows that N_n is contained in the center of G, hence $N \cap Z(G) \neq 1$.

3.5 Kolchin's theorem

Theorem 3.16 (E. Kolchin). *Let V be a finite dimensional vector space over a field K and let G be a subgroup of* $\mathbf{GL}(V)$. *Suppose that $g - 1$ is nilpotent for every $g \in G$* [2]. *Then there exists a complete flag* (see example 3 of §3.2) *of V such that G is contained in the corresponding group B_1. In particular, G is nilpotent.*

Proof. Use induction on the dimension n of V. The case $n = 0$ is trivial. Suppose that $n \geqslant 1$ and let us show first that *there exists a nonzero $x \in V$ which is G-invariant.* Finding such an x means solving a family of linear equations with coefficients in K; it

[2] Such a group is called *unipotent*.

is well known[3] that, if such a family has a nonzero solution in an extension K' of K, it has such a solution in K. Hence we may assume that K is algebraically closed. Let A be the subspace of $\mathrm{End}(V)$ generated by G. It is a subalgebra of $\mathrm{End}(V)$. There are two cases:

(i) V is a reducible A-module, i.e., there exists a G-invariant subspace $V' \subset V$ different from 0 and V. The induction hypothesis applies to V' and gives a nonzero $x \in V'$ such that $gx = x$ for all $g \in G$.

(ii) V is irreducible; in that case we have $A = \mathrm{End}(V)$ by a theorem of Burnside (cf. e.g., Bourbaki, [5], § 5.3, cor.2 to prop.4, or Lang [29], chap. XVII, cor.3.3) - this is where the assumption that K is algebraically closed is used. If $a \in G$ we have $\mathrm{Tr}(a) = n$ since the trace of a nilpotent endomorphism is 0. This implies that $n\mathrm{Tr}(aa') = \mathrm{Tr}(a)\mathrm{Tr}(a')$ for every $a, a' \in G$, hence, by linearity, for all $a, a' \in A$.
Suppose that $n > 1$ and decompose V as $V = D \oplus D' \oplus W$, with D and D' of dimension 1. Let $a : V \to D \to V$ be the projection map $(v, v', w) \mapsto (v, 0, 0)$ and define similarly $a' : V \to D' \to V$. We have $\mathrm{Tr}(a) = \mathrm{Tr}(a') = 1$ and $\mathrm{Tr}(aa') = 0$ since $aa' = 0$. This contradicts the equation $n\mathrm{Tr}(aa') = \mathrm{Tr}(a)\mathrm{Tr}(a')$. Hence the case $n > 1$ is impossible, and we have $\dim(V) = 1$, in which case G fixes V.

We have thus shown that there exists $x \in V - \{0\}$ which is G-invariant. Let $D = Kx$ be the line generated by such an x. The induction hypothesis, applied to V/D, gives a complete flag of G-stable subspaces for V/D, hence a complete flag of G-stable subspaces for V. It is clear that G is contained in the corresponding subgroup B_1.

Remark. There is a corresponding theorem for Lie algebras: if a Lie algebra $\mathfrak{g}$ acts on a finite dimensional vector space V by nilpotent endomorphisms, there exists a complete flag (V_i) of V such that $x(V_i) \subset V_{i+1}$ for every i and every $x \in \mathfrak{g}$ (*Engel's theorem*, cf. Bourbaki [8], chap.I, §4.2).

3.6 Finite nilpotent groups

Let p be a prime number.

Proposition 3.17. *Every p-group is nilpotent.*

First proof. Let P be a p-group. Then we can embed P in $\mathbf{GL}_n(\mathbf{Z}/p\mathbf{Z})$ for some sufficiently large integer n. Thus, P is contained in a p-Sylow subgroup of $\mathbf{GL}_n(\mathbf{Z}/p\mathbf{Z})$; as we have already seen, the p-Sylow subgroup is conjugate to the set B_1 of upper triangular matrices with diagonal entries equal to 1. According to the example in §3.4.1, B_1 is nilpotent, hence so is P.

Second proof. Use induction on $|P|$. We may assume that $P \neq 1$. Let P act on itself by inner automorphisms. The set of fixed points is the center $Z(P)$ of P. Since P is a

[3]Let $(x_1, \ldots, x_n)$ be a solution in K'; let $\pi : K' \to K$ be a K-linear projector $K' \to K$; then $(\pi(x_1), \ldots, \pi(x_n))$ is a solution with coefficients in K. If some x_i is nonzero, one may choose π such that $\pi(x_i)$ is nonzero.

p-group, by lemma 2.7, we have

$$|P| \equiv |Z(P)| \pmod{p},$$

and thus $Z(P) \neq 1$. The order of $P/Z(P)$ is strictly less than that of P, hence $P/Z(P)$ is nilpotent, and by cor.3.11 this shows that P is nilpotent.

Theorem 3.18. *Let G be a finite p-group.*

(1) *If H is a proper subgroup of G, then $N_G(H) \neq H$.*

(2) *Every subgroup of G of index p is normal.*

(3) *If H is a proper subgroup of G, there exists a sequence of subgroups $(H_i)_{1 \leqslant i \leqslant m}$ such that $H = H_1 \subset H_2 \subset \cdots \subset H_m = G$ with $(H_i : H_{i-1}) = p$ for $2 \leqslant i \leqslant m$.*

(4) *Every proper subgroup of G is contained in a subgroup of index p.*

(5) *If G is nontrivial, so is its center.*

Proof. (1) follows from the fact that G is nilpotent, cf. cor.3.12; it implies (2), (3) and (4). As for (5), it follows from cor.3.10.

Corollary 3.19. *Let π be a finite set of prime numbers. For every $p \in \pi$, let G_p be a finite p-group. The product $\prod_{p \in \pi} G_p$ is nilpotent.*

Conversely:

Theorem 3.20. *Let G be a finite group. The following statements are equivalent :*

(1) *G is nilpotent.*

(2) *G is a product of p-groups, for a suitable finite set of primes.*

(3) *For every prime p, G has a unique p-Sylow subgroup.*

(4) *Let p and p' be two distinct primes and let S_p (resp. $S_{p'}$) be a p-Sylow subgroup (resp. p'-Sylow subgroup) of G. Then S_p and $S_{p'}$ centralize each other* (i.e., every element of S_p commutes with every element of $S_{p'}$).

(5) *Two elements of G of relatively prime orders commute.*

Proof.

(2) $\Longrightarrow$ (1): This is corollary 3.19 proved above.

(1) $\Longrightarrow$ (3): Let S be a p-Sylow subgroup of G and let $N = N_G(S)$. Then N is its own normalizer (cf. cor.2.13). Since G is nilpotent, this implies $N = G$ by cor.3.12; thus, S is normal. Since all the p-Sylow subgroups of G are conjugate to each other, G has a unique p-Sylow subgroup.

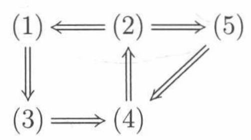
(3) $\Longrightarrow$ (4): For every prime p, let S_p be the unique p-Sylow subgroup of G. It is normal in G. If p and p' are distinct primes, $S_p \cap S_{p'} = 1$ since it is both a p-group and a p'-group; this implies (4), cf. prop.1.2.

(4) $\Longrightarrow$ (2): For every prime p, choose a p-Sylow subgroup S_p of G. The group generated by all the S_p is equal to G since its order is divisible by that of G. Consider the map $\varphi : \prod_p S_p \longrightarrow G$, given by $(s_p) \mapsto \prod_p s_p$. Since the S_p centralize one another, φ is a homomorphism. Furthermore, φ is surjective, since G is generated by the S_p. Finally, G and $\prod_p S_p$ have the same cardinality. It follows that φ is an isomorphism, which proves (2).

(2) $\Longrightarrow$ (5): Suppose that G is a product of p-groups G_p: $G = \prod_p G_p$. Let x and y be two elements of G of relatively prime orders. Then $x = (x_p)_p$ and $y = (y_p)_p$, and for every prime p we have $x_p = 1$ or $y_p = 1$. Thus $x^{-1}y^{-1}xy = (x_p^{-1}y_p^{-1}x_p y_p)_p = 1$, showing that $xy = yx$.

(5) $\Longrightarrow$ (4): This is obvious.

In summary, we have the following implications:



The theorem follows.

Corollary 3.21. *If G is nilpotent, and if d is a divisor of $|G|$, there exists a subgroup of G of order d.*

Proof. Because of (2), it is enough to prove this when G is a p-group, in which case it follows from part (4) of th.3.18.

[For a generalization of cor.3.21 to some non-nilpotent solvable groups, see chap.5, exerc.3.]

3.7 Applications of 2-groups to field theory

3.7.1. Quadratic towers, ruler and compass.

Let K be a field and let L be a finite Galois extension of K whose Galois group G is a nontrivial 2-group. According to cor.3.18, there exists a normal subgroup G' of G with $(G : G') = 2$; therefore, there exists an intermediate field L' fixed by G' which is a quadratic extension of K. If we iterate, we see that L/K is a tower of successive quadratic extensions.

Conversely, if L/K is such a tower, then its Galois closure L^{gal} is such that $\mathrm{Gal}(L^{\mathrm{gal}}/K)$ is a 2-group (see exerc.14). This provides a characterization of Galois extensions whose Galois groups are 2-groups. If $\mathrm{char}(K) \neq 2$, a quadratic extension of K is of the form

$K(\sqrt{a}) \simeq K[X]/(X^2 - a)$, where $a \in K^\times - K^{\times 2}$. (If $\mathrm{char}(K) = 2$, and if the extension is separable, replace $X^2 - a$ by $X^2 + X + a$, with $a \in K$ such that there is no $b \in K$ with $b^2 + b = a$.)

When $K = \mathbf{Q}$, this means that the numbers *constructible by ruler and compass* are the algebraic numbers contained in a Galois extension of $\mathbf{Q}$ whose Galois group is a 2-group.

Example : the impossibility of doubling the cube. The number $\sqrt[3]{2}$ is not constructible by ruler and compass, since $X^3 - 2$ is irreducible, and its degree is not a power of 2.

3.7.2. Proof that C is algebraically closed.

The proof relies on the following two properties of $\mathbf{R}$ and $\mathbf{C}$:

(1) $\mathbf{R}$ *has no algebraic extension of odd degree* > 1.

(2) $\mathbf{C}$ *has no quadratic extension.*

Property (1) follows from the fact that a polynomial with real coefficients, which is of odd degree n, has a real root (since it changes signs between $-\infty$ and $+\infty$), hence is not irreducible if $n > 1$.

Property (2) says that every complex number $z = a + ib$, with $a, b \in \mathbf{R}$, is the square of a complex number $x + iy$, i.e., that one can find $x, y \in \mathbf{R}$ with $x^2 - y^2 = a, 2xy = b$. To prove this, define

$$X = \tfrac{1}{2}(a + \sqrt{a^2 + b^2}), \quad Y = \tfrac{1}{2}(-a + \sqrt{a^2 + b^2}),$$

where the square root $\sqrt{a^2 + b^2}$ is chosen to be $\geqslant 0$. Then X and Y are $\geqslant 0$; if x, y are their positive square roots, then $x^2 - y^2 = a$ and $2xy = |b|$; in case $b < 0$, replace y by $-y$; we then have $a + ib = (x + iy)^2$.

Let us now use (1) and (2) to prove that $\mathbf{C}$ is algebraically closed. If not, $\mathbf{C}$ would have a nontrivial finite extension L. Let E be a finite Galois extension of $\mathbf{R}$ containing the field L, and let $G = \mathrm{Gal}(E/\mathbf{R})$. Since $L \neq \mathbf{C}$, we have $|G| > 2$. Let S be a 2-Sylow subgroup of G. By Galois theory, S corresponds to an extension of $\mathbf{R}$ of degree $(G : S)$, which is odd. By (1), this means $G = S$, i.e., G is a 2-group. The quadratic extension $\mathbf{C}/\mathbf{R}$ corresponds to a subgroup H of G of index 2. Since $H \neq 1$, th.3.18 shows that H has a subgroup H' of index 2. This subgroup corresponds to a quadratic extension of $\mathbf{C}$; this contradicts (2).

3.7.3. Other proofs that C is algebraically closed.

We mention two of them, which have the interest of proving much more:

a) Complex analytic proof.

Theorem (Gelfand-Mazur). *Let E be a nonzero complex Banach space, and let u be a continuous endomorphism of E. There exists $\lambda \in \mathbf{C}$ such that $u - \lambda$ is not invertible.* (Equivalently : the spectrum of u is not empty.)

Sketch of proof. If not, the function $z \mapsto (u-z)^{-1}$ would be a holomorphic map of $\mathbf{C}$ into $\mathrm{End}(E)$ tending to 0 when $|z| \to \infty$, hence would be 0, by the maximum principle.

When $E = \mathbf{C}^n, n \geqslant 1$, the theorem says that every $n \times n$ complex matrix has at least one eigenvalue; this is equivalent to $\mathbf{C}$ being algebraically closed.

b) Topological proof.

Let $f : \mathbf{C} \to \mathbf{C}$ be a function of the shape $f(z) = z^a \overline{z}^b + \varphi(z)$, where a and b are integers $\geqslant 0$, and φ is continuous. Assume that $a \neq b$ and that $\varphi(z)/|z|^{a+b} \to 0$ when $|z| \to \infty$; this is the case, for instance, when $\varphi(z)$ is a linear combination of monomials $z^c \overline{z}^d$ with $c + d < a + b$.

Theorem. *There exists $z \in \mathbf{C}$ such that $f(z) = 0$.*
[When $b = 0$ and φ is a polynomial in z of degree $< a$, this shows that $\mathbf{C}$ is algebraically closed.]

Sketch of proof. Let $X = \mathbf{P}_1(\mathbf{C}) = \mathbf{C} \cup \{\infty\} \simeq \mathbf{S}_2$. Extend f to a continuous map $X \to X$, with $f(\infty) = \infty$. This map has a topological degree $\deg(f) \in \mathbf{Z}$, which is defined by the action of f on the homology group $H_2(X, \mathbf{Z}) \simeq \mathbf{Z}$. If $t \in [0,1]$, define $f_t : X \to X$ by $f_t(z) = z^a \overline{z}^b + t\varphi(z)$ if $z \neq \infty$ and $f_t(\infty) = \infty$. Thanks to the assumption $\varphi(z)/|z|^{a+b} \to 0$, the map $[0,1] \times X \to X$ defined by $(t, z) \mapsto f_t(z)$ is continuous. Since the degree is invariant by deformation, this shows that $\deg(f_t) = \deg(f)$ for every t. For $t = 0$, we have $f_0(z) = z^a \overline{z}^b$ and it is not difficult to see that the degree of that map is $a - b$, hence is $\neq 0$. This shows that $\deg(f) \neq 0$. This implies that f is *surjective* : if not, it would factor as $X \to U \to X$, with U an open disc; since $H_2(U, \mathbf{Z}) = 0$, this would imply $\deg(f) = 0$. The surjectivity of f shows that it takes the value 0 at some point of X; such a point is not ∞ since $f(\infty) = \infty$; hence it is a point $z \in \mathbf{C}$ such that $f(z) = 0$.

The same argument applies to maps of the quaternions (or the octonions) into themselves, using the sphere $\mathbf{S}_4$ (or $\mathbf{S}_8$) instead of $\mathbf{S}_2$, and the homology group H_4 (or H_8) instead of H_2; the only assumption is the existence of a dominant monomial with a nonzero topological degree. Note that, for the quaternions, which are not commutative, the monomial $z^a \overline{z}^b$ can be replaced by something more complicated, such as, for instance, $z\overline{z}jz^3k\overline{z}^5i$, which has total degree 10 and topological degree -2. For octonions, which are not associative, parentheses have to be inserted; a monomial such as $(az)(z(b\overline{z}))$ is not the same as $((a(zb))z)\overline{z}$.

3.8 Abelian groups

Every abelian group is nilpotent; according to th.3.20, every finite abelian group is a product of abelian p-groups. We can refine this decomposition thanks to the well-known:

Theorem 3.22. *Every finite abelian p-group is a product of cyclic groups.*

Note that, if G is a finite abelian p-group, there exists an integer n such that $p^n x = 0$ for all $x \in G$; hence G can be viewed as a $\mathbf{Z}/p^n\mathbf{Z}$-module. Theorem 3.22 is thus a special case of the following one, where there is no finiteness assumption:

Theorem 3.23. *Every $\mathbf{Z}/p^n\mathbf{Z}$-module is a direct sum of cyclic modules (isomorphic to $\mathbf{Z}/p^i\mathbf{Z}$ for some $i \leqslant n$).*

Proof. Let M be a $\mathbf{Z}/p^n\mathbf{Z}$-module and let V be the $\mathbf{F}_p$-vector space M/pM.
For $i = 0, \dots, n$, let M_i be the set $\{x \in M \mid p^i x = 0\}$. We have:

$$M_0 = 0 \subset M_1 \subset \cdots \subset M_n = M.$$

If V_i is the image of M_i in V, then

$$V_0 = 0 \subset V_1 \subset \cdots \subset V_n = V.$$

Let S be a basis of V that is adapted to the (V_i) (i.e., $S_i = S \cap V_i$ is a basis of V_i for every i); such a basis exists: choose first a basis of V_1, then a basis of V_2/V_1 which is lifted to V_2, etc.
If $s \in S$, denote by $i(s)$ the smallest i for which $s \in S_i$ and choose a representative $\bar{s} \in M_{i(s)}$ of s. We have $p^{i(s)}\bar{s} = 0$. Let $M' = \bigoplus_{s \in S} \mathbf{Z}/p^{i(s)}\mathbf{Z}$ and define a homomorphism $\varphi : M' \to M$ by $(n_s)_{s \in S} \mapsto \sum_{s \in S} n_s \bar{s}$. This map is an isomorphism. Indeed:

φ is surjective: Let H be the submodule of M generated by the $\bar{s}$. The projection map $H \to V$ is surjective, since its image contains S. Thus, $M = pM + H$. This implies $M = p(pM + H) + H = p^2 M + H$, and by iteration $M = p^i M + H$ for every i; for $i = n$, this gives $M = H$.

φ is injective: Let $(n_s) \in M'$ be such that $\sum_{s \in S} n_s \bar{s} = 0$ in M. Let us show that n_s is divisible by p^i for every integer $i \geqslant 0$ (thus $n_s = 0$). Use induction on i. For $i = 0$, there is nothing to prove. Suppose that this holds up to k. Then $n_s = 0$ if $i(s) \leqslant k$ and we only need to look at the s for which $i(s) \geqslant k + 1$. By assumption, $\sum_{i(s) \geqslant k+1} n_s \bar{s} = 0$. Write $n_s = p^k m_s$ with $m_s \in \mathbf{Z}/p^{i(s)}\mathbf{Z}$. We have $p^k \sum_{i(s) \geqslant k+1} m_s \bar{s} = 0$, which implies $\sum_{i(s) \geqslant k+1} m_s \bar{s} \in M_k$; hence, by projection, we have $\sum_{i(s) \geqslant k+1} m_s s \in V_k$. By the choice of S and the definition of $i(s)$, we have $m_s \equiv 0 \pmod{p}$. Therefore, p^{k+1} divides n_s. This completes the induction.

3.9 The Frattini subgroup

Let G be a finite group. The intersection of all the maximal subgroups[4] of G is called the **Frattini subgroup** of G, and is denoted by $\Phi(G)$. It is a characteristic subgroup of G. Its main property is:

[4] A subgroup H of G is called **maximal** if it is maximal among the proper subgroups of G, cf. chap.1, exerc.16.

Proposition 3.24. *Let $S \subset G$ and let H be the subgroup of G generated by S. We have $H = G$ if and only if $H.\Phi(G) = G$, i.e., if S generates $G/\Phi(G)$.*

Proof. One direction is obvious. For the nontrivial direction, if $H.\Phi(G) = G$ and $H \neq G$, there exists a maximal subgroup H' of G containing H; by definition, $\Phi(G) \subset H'$. It follows that $G \subset H'$, which is absurd.

Remark. This shows that the elements of $\Phi(G)$ are " non-generators " of G: if a set S generates G, so does $S - S \cap \Phi(G)$.

Theorem 3.25. *The group $\Phi(G)$ is nilpotent.*

Proof. Let p be a prime number and let S be a p-Sylow subgroup of $\Phi(G)$. By part (4) of prop.2.11, we have $G = \Phi(G).N_G(S)$. According to prop.3.24, this implies $N_G(S) = G$; hence S is normal in G, and *a fortiori* normal in $\Phi(G)$. Therefore, S is the unique p-Sylow subgroup of $\Phi(G)$. Since this is true for every p, th.3.20 (3) shows that $\Phi(G)$ is nilpotent.

In the case where G is nilpotent, there is a simple characterization of $\Phi(G)$:

Theorem 3.26. *If G is nilpotent, $\Phi(G)$ is the intersection of the normal subgroups of G of prime index.*

Proof. This follows from the characterization of the maximal subgroups given in cor.3.12.

Theorem 3.27. *If G is a p-group, then $\Phi(G) = (G,G).G^p$; it is the intersection of the normal subgroups of G of index p.*

Proof. The second assertion is a special case of the theorem above. As for the first one, the inclusion $(G,G).G^p \subset \Phi(G)$ is clear. Conversely, if $g \notin (G,G).G^p$, its image v in the $\mathbf{F}_p$-vector space $V = G/(G,G).G^p$ is nontrivial; by choosing a linear map $\ell : V \to \mathbf{F}_p$ such that $\ell(v) \neq 0$, we obtain a homomorphism $\varphi : G \to V \to \mathbf{F}_p$ such that $\varphi(g) \neq 0$, hence $g \notin \Phi(G)$.

Corollary 3.28. *Let G be a p-group and let S be a subset of G. If the image of S in $G/(G,G).G^p$ generates that group, then S generates G.*

Thus, if G is a p-group, the minimal cardinal of a generating set of G is $\dim_{\mathbf{F}_p} G/\Phi(G)$; it is called the **rank** of G.

Application : automorphisms of a p-group.

Let G be a finite p-group of rank r, and let $V_G = G/\Phi(G)$. Every automorphism of G defines an automorphism of V_G, i.e., an element of $\mathrm{GL}(V_G) \simeq \mathrm{GL}_r(\mathbf{F}_p)$. Let P_G be the kernel of $\mathrm{Aut}(G) \to \mathrm{GL}(V_G)$. We have an exact sequence:

$$1 \to P_G \to \mathrm{Aut}(G) \to \mathrm{GL}(V_G).$$

Proposition 3.29. (1) *P_G is a p-group.*
(2) *Let p^m be the order of $\Phi(G)$. We have $s^{p^m} = 1$ for every $s \in P_G$.*

Proof. It is enough to prove (2). We do it by induction on m. If $m = 0$, then $G = V$ and $s = 1$ by assumption. Assume that $m > 0$, i.e., $\Phi(G) \neq 1$. By lemma 3.15, the abelian group $A = \Phi(G) \cap Z(G)$ is nontrivial. Let B be the subgroup of A made up of the elements $a \in A$ such that $a^p = 1$. The group A is a nontrivial characteristic subgroup of G. Let $G' = G/A$. Since $A \subset \Phi(G)$, we have $\Phi(G') = \Phi(G)/A$ and $V_{G'} \simeq V_G$. Hence s acts trivially on $V_{G'}$. Since the order $p^{m'}$ of $\Phi(G')$ is $< p^m$, the induction assumption show that the automorphism $t = s^{p^{m'}}$ acts trivially on G'. This means that, if $g \in G$, we have $t(g) = g.e(g)$ with $e(g) \in A$. Since $A \subset Z(G)$, we have $t(g)e(g)t(g')e(g') = t(gg').e(g)e(g')$ for every $g, g' \in G$, hence $e : G \to A$ is a homomorphism. This implies that $e(g^p) = 1$ for every g, and also that $e(g) = 1$ for every $g \in \Phi(G)$ (because A is a product of copies of $\mathbf{Z}/p\mathbf{Z}$, and every homomorphism of G into $\mathbf{Z}/p\mathbf{Z}$ is trivial on $\Phi(G)$, cf. th.3.27). One checks by induction on n that $t^n(g) = g.e(g)^n$ for every $n \geqslant 0$ (use the fact that $t(a) = a$ for every $a \in A$). By taking $n = p$, this gives $t^p(g) = g.e(g)^p = g$ for every g. Hence $t^p = 1$, i.e., $s^{p^{m'+1}} = 1$; since $m > m'$, the induction assumption shows that $s^{p^m} = 1$.

Corollary 3.30. *If C is a subgroup of $\mathrm{Aut}(G)$ of order prime to p, then C acts faithfully on $V_G = G/\Phi(G)$, and its order divides $\prod_{i=1}^{r}(p^i - 1)$.*

Proof. The first assertion follows from $C \cap P_G = 1$. It implies that $|C|$ divides the order of $\mathrm{GL}(V_G)$, which is $p^{r(r-1)/2}\prod_{i=1}^{r}(p^i - 1)$; since $|C|$ is prime to p, $|C|$ divides $\prod_{i=1}^{r}(p^i - 1)$.

3.10 Characterizations using subgroups generated by two elements.

Let us see whether some property of the subgroups of G generated by two elements implies the same property for G itself. Here is a simple example:

Proposition 3.31. *Let G be a group (resp. a finite group). Suppose that every subgroup of G generated by two elements is abelian (resp. nilpotent). Then G is abelian (resp. nilpotent).*

Proof. Let $x, y \in G$. The subgroup $\langle x, y\rangle$ generated by x and y is abelian, therefore $xy = yx$, hence G is abelian. If G is a finite group and $\langle x, y\rangle$ is nilpotent for every x, y, characterization (5) of th.3.20 implies that G is nilpotent.

[In the nilpotent case the finiteness hypothesis cannot be deleted, see exerc.9.]

The next question is whether the analogous statement for *solvable* finite groups is true. J.G. Thompson has shown that the answer is "yes" but the proof is much more difficult. To explain its principle, let us first make a definition: a finite group G is called **minimal simple** if G is simple nonabelian and every proper subgroup of G is solvable.

Lemma 3.32. *If a finite group G is not solvable, there exist a subgroup H of G and a normal subgroup K of H such that H/K is a minimal simple group.*

Example. If $G = \mathrm{GL}_2(\mathbf{F}_5)$, take $H = \mathrm{SL}_2(\mathbf{F}_5)$ and $K = \{\pm 1\}$, so that $H/K \simeq \mathcal{A}_5$, which is a minimal simple group.

Proof of the lemma. Let H be a minimal nonsolvable subgroup of G and let K be a maximal normal subgroup of H distinct from H. The group K is solvable, since it is strictly contained in H. The quotient H/K is simple, because K is maximal among the proper normal subgroups, and it is nonabelian, otherwise H would be solvable. Moreover, H/K is a minimal simple group: every proper subgroup of H/K is a quotient of a proper subgroup of H, hence is solvable.

Proposition 3.33. *The following two statements are equivalent :*
(1) *Every minimal simple group can be generated by two elements.*
(2) *Every finite group, all of whose 2-generated subgroups are solvable, is also solvable.*

Proof of (2) $\Longrightarrow$ (1). Suppose that (2) holds. Let G be a minimal simple group. If $\langle x, y\rangle \neq G$ for all pairs $(x, y) \in G \times G$, then $\langle x, y\rangle$ is solvable since it is a proper subgroup of G. Now, according to (2), G is solvable. Contradiction.

Proof of (1) $\Longrightarrow$ (2). Suppose that (1) holds. If a group G is not solvable, choose H and K as in lemma 3.32. The group H/K is a minimal simple group; therefore, it is generated by two elements; one can then find a subgroup H' of H, which is generated by two elements and is such that $H = H'K$. The group H' is solvable by hypothesis; since $H' \to H/K$ is surjective, H/K is solvable. Contradiction.

The problem of proving that (2) is true is thus reduced to the following task: find all the minimal simple groups and check that each of them can be generated by two elements. This was done by Thompson, who showed in a long series of papers [79] that a minimal simple group is isomorphic to one - and only one - of the following groups (which can each be generated by two elements):

- $\mathbf{PSL}_2(\mathbf{F}_p)$, p prime > 3, $p \not\equiv \pm 1 \pmod 5$,
- $\mathbf{PSL}_2(\mathbf{F}_{2^p})$, p prime > 2,
- $\mathbf{PSL}_2(\mathbf{F}_{3^p})$, p prime > 2,
- $\mathbf{PSL}_3(\mathbf{F}_3)$,
- The Suzuki groups[5] $\mathbf{Sz}(2^p)$ for p prime > 2.

[5]The Suzuki groups $\mathbf{Sz}(q)$ are twisted forms of $\mathbf{SO}_5$, associated with the powers q of 2 with odd exponent: 2, 8, 32, ...; they are simple for $q \geqslant 8$, see Wilson [39], §4.2. The order of $\mathbf{Sz}(q)$ is $q^2(q^2+1)(q-1)$, which is not divisible by 3; according to CFSG, these groups are the only nonabelian simple groups having that property.

Remarks

1. One may ask whether a nonabelian simple group that is minimal in the naive sense (i.e., that does not contain a proper subgroup that is both simple and nonabelian) is minimal in the sense defined above. The answer has recently been shown to be "yes", assuming CFSG, see Barry-Ward [43].

2. It is also a consequence of CFSG that every finite simple group (minimal or not) can be generated by two elements, cf. Gorenstein [21], 1.47.

3. A proof of (1) and (2) independent of Thompson's classification of minimal simple groups was given later by P. Flavell [56].

3.11 Exercises

1. (*Jordan.*) Let G be a solvable finite group, and let H be a maximal subgroup of G. Show that $(G : H)$ is a power of a prime number.
   [Hint: choose a nontrivial normal p-subgroup N of G, cf. cor.3.3, and consider separately the case where $N \subset H$ and the case where $N \not\subset H$.]

2. Let G be a finite group and let N be a normal subgroup of G. Show the equivalence of :
   (i) $N \supset D^{\infty}G$.
   (ii) G/N is solvable.
   (iii) There exist prime numbers $p_1, ..., p_n$ such that $N \supset O^{p_1}(O^{p_2}(\dots(O^{p_n}(G)\dots)))$.
   [For the definition of $O^p(G)$, see exerc.3 of chap.2.]

3. (*p-nilpotent groups.*) Let G be a finite group, let p be a prime number and let S be p-Sylow subgroup of G. Prove the equivalence of the following properties:
   a) There exists a surjective homomorphism $G \to S$.
   b) There exists a homomorphism $G \to S$ whose restriction to S is id_S.
   c) The elements of G of order prime to p make up a subgroup of G.
   d) There exists a normal subgroup of G of order $(G : S)$.
   e) The group S has a normal complement in G (in the sense of exerc.11 of chap.2).
   f) The group G is the semidirect product (cf. §4.3) of a group of order prime to p by a p-group.
   If these properties hold, G is called a *p-nilpotent group.* Show that G is nilpotent if and only if it is p-nilpotent for every p.

4. Let $x, y \in G$. Show that $xyx^{-1}y^{-1} \equiv x^{-1}y^{-1}xy \mod C^3(G)$.

5. (*Small p-groups.*) Let G be a finite p-group.
   a) If $|G| = p$ or p^2, show that G is abelian.
   b) Suppose that $|G| = p^3$ and G is nonabelian. Show that $Z(G)$ has order p, and that $V = G/Z(G)$ is an $\mathbf{F}_p$-vector space of dimension 2. Moreover:
   b$_1$) Assume $p = 2$. Show that G is either a dihedral group of order 8, or a quaternion group of order 8, depending on whether it contains one, or three, cyclic subgroups of order 4.
   [Hint: If $x \in G$, then x^2 belongs to $Z(G) \simeq \mathbf{F}_2$ and depends only on the image of

$x \in V$. This defines a quadratic form $q : V \to \mathbf{F}_2$. Show that this form is not additive, and that, by choosing suitable coordinates (x, y) in V, we have either $q(x, y) = xy$ or $q(x, y) = x^2 + xy + y^2$. Show that G is determined by q.]
Show that a 2-Sylow of $\mathrm{SL}_3(\mathbf{F}_2)$ (resp. of $\mathrm{SL}_2(\mathbf{F}_3)$) is a dihedral group (resp. a quaternion group) of order 8.
b$_1$) Assume $p \geqslant 3$. Show that there are two possibilities for G, depending on whether G contains an element of order p^2 or not. When such an element exists, G is a semidirect product of a cyclic group of order p by a cyclic group of order p^2. When it does not exist, G is isomorphic to a p-Sylow of $\mathrm{GL}_3(\mathbf{F}_p)$.
[Hint: if there is no element of order p^2, show that one can choose three elements x, y, z of G, of order p, with $z \in Z(G)$, such that $xy = zyx$.]

6. (*Iwasawa's simplicity criterion.*)
Let G, M, U be groups with $G \supset M \supset U$, and U normal in M. Assume:
a) $G^{\mathrm{ab}} = 1$;
b) U is solvable;
c) M is a maximal subgroup of G;
d) G acts faithfully on G/M;
e) The conjugates of U generate G.
Show that G is simple.
[Hint: Let N be a proper nontrivial normal subgroup of G. By d), N is not contained in M and by c) we have $G = MN$. Let $G' = G/N$ and let U' be the image of U in G'. Since $M \to G'$ is surjective, U' is normal in G'; by e) we have $U' = G'$. By b), this shows that G' is solvable, hence $G'^{\mathrm{ab}} \neq 1$, which contradicts a).]

7. (*Simplicity of* $\mathrm{PSL}_n(K)$.) Let K be a field, and let $G = \mathrm{PSL}_n(K)$, with $n \geqslant 2$; assume that $|K| > 3$ if $n = 2$. Choose a 1-dimensional subspace D of K^n. Let $\widetilde{M}$ be the subgroup of $\mathrm{SL}_n(K)$ stabilizing D, and let $\widetilde{U}$ be the subgroup of $\widetilde{M}$ made up of the elements which act trivially on D and on K^n/D. Let M and U be the images in G of $\widetilde{M}$ and $\widetilde{U}$. Show that (G, M, U) have the properties a), ...,e) of exerc.6, hence that $\mathrm{PSL}_n(K)$ is simple.
[Hint for a) and e): Show first that $\mathrm{SL}_n(K)$ is generated by the elementary matrices of the form $1+\lambda e_{ij}$, with $\lambda \in k$ and $i \neq j$, cf. e.g. Huppert [25], II.6.7 or Lang [29], XIII.9.1. These matrices are conjugate to elements of U; this proves a). As for e), show that every $1 + \lambda e_{ij}$ is a commutator in $\mathrm{SL}_n(K)$ (when $n = 2$, use the assumption $|K| > 3$).]
[Hint for c): show that G acts 2-transitively on G/M, which is the projective space $\mathbf{P}_{n-1}(K)$; this implies that M is a maximal subgroup of G.]

8. (*Generalization of the triangular matrix group.*) Let $A = A_0 \supset A_1 \supset \cdots$ be a decreasing sequence of normal subgroups of a group A. Let $G \subset \mathrm{Aut}A$ be such that $g(A_i) = A_i$ for every i. If $n \geqslant 0$, let G_n be the set of all $g \in G$ such that $a^{-1}g(a) \in A_{i+n}$ for every $i \geqslant 0$ and every $a \in A_i$.
a) Show that $G = G_0 \supset G_1 \supset \cdots$ is a decreasing sequence of normal subgroups of G. Suppose that all the A_i/A_{i+1} are abelian. Show that $(G_1, G_n) \subset G_{n+1}$ for every n, hence G_1/G_n is nilpotent of nilpotency class $< n$.
b) Suppose that $(A_i)_{i \geqslant 1}$ is a central filtration of A_1. Show that $(G_i)_{i \geqslant 1}$ is a central filtration of G_1.

9. a) Construct an infinite sequence $(G_1, G_2, \dots)$ of finite nilpotent groups such that the nilpotency class of G_n tends to ∞ with n.

b) Let G be the subgroup of $\prod_n G_n$ made up of the sequences (x_n) such that $x_n = 1$ for all large enough n. Show that G is not nilpotent, but that every finitely generated subgroup of G is nilpotent.

10. Let M be a $\mathbf{Z}/n\mathbf{Z}$-module, $n \geqslant 1$, and let C be a cyclic subgroup of M of order n. Show that C is a direct summand, i.e., that there exists a subgroup N of M such that $M = C \oplus N$.

11. (*Invariants of a $\mathbf{Z}/p^n\mathbf{Z}$-module.*) Let M be a $\mathbf{Z}/p^n\mathbf{Z}$-module. Choose a splitting of M as a direct sum of cyclic modules M_λ. For every i with $1 \leqslant i \leqslant n$, let $\mathbf{c}_i$ be the cardinal of the set of λ such that $|M_\lambda| = p^i$. Show that $\mathbf{c}_i$ is independent of the choice of the splitting. Hence M is defined, up to isomorphism, by the family $(\mathbf{c}_1, \ldots, \mathbf{c}_n)$.

12. (*A variant of Kolchin's theorem in dimension* 2.) Let K be a field and let G be a finite[6] subgroup of $\mathrm{GL}_2(K)$. Assume that $\det(g-1) = 0$ for every $g \in G$. Show that G is conjugate to a subgroup of either $\begin{pmatrix} 1 & 0 \\ * & * \end{pmatrix}$ or $\begin{pmatrix} * & 0 \\ * & 1 \end{pmatrix}$.
[Hint: Let $N = G \cap \mathrm{SL}_2(K)$. Distinguish two cases:
a) $N = 1$; in that case the determinant map $\chi = \det : G \to K^\times$ is injective; hence G is cyclic, and the result follows from the hypothesis applied to a generator of G.
b) $N \neq 1$, which is possible only if the characteristic p of K is > 0. In that case N is a nontrivial p-group, and hence fixes a unique line D in $V = K^2$. The action of G on D and on V/D is given by two homomorphisms $\alpha, \beta : G \to K^\times$. The hypothesis on G implies that G is the union of the two subgroups $\operatorname{Ker}\alpha$ and $\operatorname{Ker}\beta$. By exerc.4 of chap.1, this implies that either α or β is trivial, as wanted.]

13. (*Supersolvable groups.*) Let G be a finite group. Show that the following two properties are equivalent:
(i) There exists a filtration (G_i) of G such that the G_i are normal in G, and the $\mathrm{gr}_i(G)$ are cyclic.
(ii) The group G is solvable and there exists a Jordan-Hölder filtration (G_i) of G such that every G_i is normal in G.
A group having these properties is called **supersolvable**. A finite nilpotent group is supersolvable. A subgroup, a quotient and a central extension of a supersolvable group are supersolvable. If G has a normal cyclic subgroup N such that G/N is supersolvable, then G is supersolvable.
In what follows, G is assumed to be supersolvable.
a) Let H be a maximal subgroup of G. Show that the index of H in G is a prime number.
[Hint: choose a normal subgroup N of G of prime order; use induction on $|G|$ if $N \subset H$; if $N \cap H = 1$, use that $HN = G$, hence $(G : H) = |N|$.]
b) Suppose that G is not abelian. Show that there exists a normal abelian subgroup of G that is not contained in the center of G.
[Hint: use a normal nontrivial cyclic subgroup of $G/Z(G)$.]
c) Show that $D(G)$ is nilpotent.
[Hint: let $(G_i)_{0 \leqslant i \leqslant n}$ be a Jordan-Hölder filtration of G; let H be the subgroup of G made up of the elements h such that int_h acts trivially on each G_i/G_{i+1}; use exerc.8 to prove that $H/Z(G)$ is nilpotent; hence H is nilpotent; show that $D(G) \subset H$.]

---

[6]The finiteness assumption is not necessary. This can be seen by applying Bourbaki [5], §20, cor.2 to the group algebra $K[G]$.

d) Let $\mathcal{P}_G$ denotes the set of all prime numbers dividing $|G|$. Let $p \in \mathcal{P}_G$ be such that $q \in \mathcal{P}_G \implies q \not\equiv 1 \pmod{p}$. Show that G has a normal subgroup of order p.
[Hint: use induction on $|G|$; choose a normal subgroup N of prime order q; in case $q \neq p$, the induction shows the existence of a normal subgroup M of order pq with $N \subset M$; use the hypothesis $q \not\equiv 1 \pmod{p}$ to show that M splits uniquely as $M = N \times N'$ with $|N'| = p$, and that N' is normal in G.]
e) Choose a total order $q \prec p$ on $\mathcal{P}_G$ such that $q \prec p \implies q \not\equiv 1 \pmod{p}$ (the usual order $q < p$ has that property). Use d) to show that G has a Jordan-Hölder filtration $(G_i)_{0 \leqslant i \leqslant n}$ such that $(G_i : G_{i+1}) \prec (G_j : G_{j+1})$ implies $i \leqslant j$ (i.e., the function $i \mapsto (G_i : G_{i+1})$ is nondecreasing). If p (resp. p') is the largest (resp. the smallest) element of $\mathcal{P}_G$ for the relation $\prec$, show that G has a unique p-Sylow subgroup (resp. that G is p'-nilpotent, cf. exerc.3).
[More properties of supersolvable groups can be found in: chap.5, exerc.2 and 3; chap.7, exerc.15; chap.8, exerc.12; chap.9, exerc.9.]

14. (*Field towers.*) a) Let G be a finite group, and let $H_1, \ldots, H_n$ be a family of subgroups of G, with $G = H_1 \supset H_2 \supset \cdots \supset H_n$. Assume that the action of G on G/H_n is faithful, i.e., that the intersection of the conjugates of H_n is 1. Let N be an integer such that $(H_i : H_{i+1}) \leqslant N$ for $i = 1, \ldots, n-1$. Show that the prime divisors of $|G|$ are $\leqslant N$.
[Hint: suppose that G contains an element g of prime order $> N$. Show by induction on i that g belongs to all the conjugates of H_i; this gives a contradiction for $i = n$.]
In particular, G is a 2-group if $N = 2$.
b) Let K a field, and let $K = K_1 \subset K_2 \subset \cdots \subset K_n$ be a tower of quadratic separable extensions of K inside an algebraic closure of K. Let L be the smallest Galois extension of K containing K_n. Show that $\mathrm{Gal}(L/K)$ is a 2-group.
[Hint: apply a) to $G = \mathrm{Gal}(L/K)$ and $H_i = \mathrm{Gal}(L/K_i)$, with $N = 2$.]

15. Let $1 \to A \to G \to B \to 1$ be an exact sequence of groups. Assume that B is simple nonabelian and that $\mathrm{Out}(A)$ is solvable. Show that $G = A.C_G(A)$. If $Z(A) = 1$, show that $G \simeq A \times B$.

16. (*Direct products of nonabelian simple groups.*) Let G be a group, and let (N_i) be a finite family of normal subgroups of G, with $N_i \cap N_j = 1$ if $i \neq j$. Assume that the N_i generate G, and that they are simple nonabelian.
a) Show that G is the direct product of the N_i.
b) Show that every nontrivial normal subgroup of G contains one of the N_i. In particular, the N_i are the minimal nontrivial normal subgroups of G.
c) Show that every automorphism of G permutes the N_i.
d) Suppose that $\mathrm{Out}(N_i)$ is solvable[7] for every i. Show that $\mathrm{Out}(G)$ is solvable if and only if there are at most four N_i which are isomorphic to each other.
[Hint: use the fact that the symmetric group $\mathcal{S}_n$ is solvable if and only if $n \leqslant 4$.]

17. (*Groups whose Jordan-Hölder quotients are nonabelian.*) Let $(H_i)_{i=0,\ldots,n}$ be a Jordan-Hölder filtration of a group G, and let $G_i = H_{i-1}/H_i$ be the corresponding simple subquotients.

a) Assume:
i) For every $i = 1, \ldots n$, the group G_i is nonabelian and $\mathrm{Out}(G_i)$ is solvable.

[7] It follows from CFSG that this is always true if N_i is finite, cf. Gorenstein [21], th.1.46 and [22], vol.3, th.7.1.1.

ii) At most four of the G_i are isomorphic to each other.
Show that:
iii) G is isomorphic to $G_1 \times \cdots \times G_n$.
[Hint: use the two exercises above.]

b) Assume only condition i). Show that iii) holds if $|G| < 60^7$, provided $|G| \neq 60^6$.
[Hint: use the fact that the two smallest nonabelian simple groups have order 60 and 168, cf. §7.7; use also the inequality $168^5 > 60^6$.]
Construct an example (resp. two distinct examples) showing why 60^6 (resp. 60^7) has to be excluded.

18. (*Torsion in nilpotent groups.*) Let G be a nilpotent group.
a) Show that G is finite $\Longleftrightarrow$ G^{ab} is finite $\Longleftrightarrow$ G has finite length.
[Hint: if G^{ab} is finite, show that the Lie algebra $\mathrm{gr}(G)$ is finite.]
b) Show that the elements of G of finite order make up a subgroup of G.
[Hint: if x, y have finite order, show that xy has finite order by applying a) to the subgroup of G generated by x and y.]

19. (*Minimality of* $\mathrm{PSL}_2(\mathbf{F}_q)$.) Show that $\mathrm{PSL}_2(\mathbf{F}_q)$ is a minimal simple group only for the values of q mentioned in §3.10.
[Hint: use the fact that this group contains $\mathrm{PSL}_2(\mathbf{F}_{q'})$ if q is a power of q', and that it contains $\mathcal{A}_5$ if $q \equiv \pm 1 \pmod 5$, cf. §10.2.]

Chapter 4

Group extensions

4.1 Cohomology groups

Before discussing group extensions, we recall a few facts about group cohomology; for more information, especially on the point of view "derived functors", we refer the reader to Cartan-Eilenberg [13], Brown [11] and Lang [30].

Let G be a group (written multiplicatively) and let A be a G-module (i.e., an abelian group written additively on which G acts by automorphisms). We write sa for the transform of $a \in A$ by $s \in G$. We have

$$\begin{aligned} (st)a &= s(ta), \\ 1a &= a, \\ s(a_1 + a_2) &= sa_1 + sa_2, \end{aligned}$$

for all $s, t \in G$ and all $a, a_1, a_2 \in A$.

Here are some examples:

1. The trivial action of a group G on A, i.e., $sa = a$ for all $s \in G$ and all $a \in A$.
2. If L is a Galois extension of a field K, then $G = \mathrm{Gal}(L/K)$ acts by automorphisms on the additive group L and on the multiplicative group $L^\times$.

Definition 4.1. *Let n be an integer $\geqslant 0$. An **n-cochain**, or a **cochain of degree** n, on G with values in A is a function of n variables in G with values in A:*

$$\begin{aligned} f : G \times G \times \cdots \times G &\longrightarrow A, \\ (s_1, s_2, \ldots, s_n) &\longmapsto f(s_1, s_2, \ldots, s_n). \end{aligned}$$

The set of all cochains, with addition induced from A, forms an abelian group, which we denote by $C^n(G, A)$.

Examples. (1) $n = 0$: a function of zero variable with values in A is an element of A. Thus, $C^0(G, A) = A$.

(2) $n = 1$: $C^1(G, A) =$ maps from G to A.

(3) $n = 2$: $C^2(G, A) =$ maps from $G \times G$ to A.

Definition 4.2. *Let $f \in C^n(G, A)$. The* ***coboundary*** *of f, denoted by df, is the element of $C^{n+1}(G, A)$ defined by the following formula :*

$$\begin{aligned} df(s_1, \ldots, s_n, s_{n+1}) &= s_1 f(s_2, \ldots, s_{n+1}) + \sum_{i=1}^{n} (-1)^i f(s_1, \ldots, s_{i-1}, s_i s_{i+1}, s_{i+2}, \ldots, s_{n+1}) \\ &\quad + (-1)^{n+1} f(s_1, \ldots, s_n). \end{aligned}$$

Let us look at some low-degree examples:

(1) $d: C^0(G, A) \longrightarrow C^1(G, A)$. Let $a \in A = C^0(G, A)$. We have $da(s) = sa - a$. Note that $da = 0$ if and only if a is fixed by all the elements of G.

(2) $d: C^1(G, A) \longrightarrow C^2(G, A)$. Let f be a 1-cochain. We have

$$df(s, t) = sf(t) - f(st) + f(s).$$

(3) $d: C^2(G, A) \longrightarrow C^3(G, A)$. Let f be a 2-cochain. We have

$$df(u, v, w) = uf(v, w) - f(uv, w) + f(u, vw) - f(u, v).$$

Theorem 4.1 (Basic Formula). *We have $d \circ d = 0$. In other words, the following composition is zero :*

$$C^n(G, A) \xrightarrow{d} C^{n+1}(G, A) \xrightarrow{d} C^{n+2}(G, A)\,.$$

Proof. We prove this for $n = 0$ and $n = 1$; for the general case, see exerc.1. For $n = 0$, and $a \in A = C^0(G, A)$, we have $da(s) = sa - a$. It follows that

$$\begin{aligned} dda(s, t) &= sda(t) - da(st) + da(s) \\ &= s(ta - a) - (sta - a) + (sa - a) \\ &= 0. \end{aligned}$$

Now for $n = 1$, let $f \in C^1(G, A)$. We have

$$\begin{aligned} ddf(u, v, w) &= u\,df(v, w) - df(uv, w) + df(u, vw) - df(u, v) \\ &= u\big(vf(w) - f(vw) + f(v)\big) - \big(uvf(w) - f(uvw) + f(uv)\big) \\ &\quad + \big(uf(vw) - f(uvw) + f(u)\big) - \big(uf(v) - f(uv) + f(u)\big) \\ &= 0. \end{aligned}$$

Definition 4.3. *An n-cochain f is called an* ***n-cocycle*** *if $df = 0$. It is called an* ***n-coboundary*** *if there exists an $(n-1)$-cochain g such that $f = dg$.*

According to th.4.1, every n-coboundary is an n-cocycle. We write $Z^n(G,A)$ to denote the group of n-cocycles and $B^n(G,A)$ the group of n-coboundaries.

The quotient group $Z^n(G,A)/B^n(G,A)$ is denoted by $H^n(G,A)$ and is called the $n^{\mathbf{th}}$ **cohomology group of G with values in A**. Two n-cocycles are said to be **cohomologous** if they define the same cohomology class in $H^n(G,A)$, i.e., if their difference is a coboundary.

The case where G is trivial. If $G=1$, we have $C^n(G,A)=A$ for every $n\geqslant 0$, and the coboundary map $d:C^n(G,A)\to C^{n+1}(g,A)$ is 0 if n is even and is the identity map $A\to A$ if n is odd. Hence $H^0(G,A)=A$, and $H^n(G,A)=0$ for $n>0$.

Low-dimensional examples.

1. For $n=0$, by convention, we have $B^0=0$. Let A^G denote the group of elements in A fixed by all the elements of G. We have seen that

$$da=0\iff a\in A^G;$$

hence, $H^0(G,A)=A^G$.

2. For $n=1$, an element in $Z^1(G,A)$ is a function $f:G\to A$ such that $df(s,t)=0$ for all $s,t\in G$, i.e.,

$$f(st)=sf(t)+f(s). \tag{4.1}$$

Such a function is called a **crossed homomorphism**; we have $f(1)=0$, as is seen by applying the equation above to $s=t=1$.

If G acts trivially on A, we have $sf(t)=f(t)$ and f is a homomorphism of G into A; since $B^1(G,A)=0$, we have

$$H^1(G,A)=\mathrm{Hom}(G,A).$$

3. For $n=2$, a function $f:G\times G\to A$ is a 2-cocycle if

$$uf(v,w)-f(uv,w)+f(u,vw)-f(u,v)=0\quad\text{for all } u,v,w\in G. \tag{4.2}$$

Such a function is called a **factor set**; it is said to be **normalized** if $f(1,1)=0$. By using the equation above with (u,v,w) replaced by $(1,1,x)$ and $(x,1,1)$, we obtain

$$f(1,x)=f(1,1)\quad\text{and}\quad f(x,1)=xf(1,1)\quad\text{for every } x\in G. \tag{4.3}$$

Hence $f(1,x)=f(x,1)=0$ if f is normalized.

Lemma 4.2. *Every factor set is cohomologous to a normalized factor set.*

Proof. Let f be a factor set. Choose $c:G\to A$ such that $c(1)=-f(1,1)$. Then $f+dc$ is a normalized factor set which is cohomologous to f.

4.2 A vanishing criterion for the cohomology of finite groups

Let G be a finite group and let A be a G-module. Let $m = |G|$.

Theorem 4.3. *If $x \in H^n(G, A)$ with $n \geqslant 1$, then $mx = 0$.*

Proof. Let $f \in Z^n(G, A)$ be an n-cocycle in the class x. Let us show that mf is a coboundary. Since f is a cocycle, we have:

$$0 = s_1 f(s_2, \ldots, s_{n+1}) - f(s_1 s_2, s_3, \ldots, s_{n+1}) + \cdots + (-1)^n f(s_1, \ldots, s_n s_{n+1}) + (-1)^{n+1} f(s_1, \ldots, s_n).$$

Let $F_1(s_1, \ldots, s_{n-1}) = \sum_{s \in G} f(s_1, \ldots, s_{n-1}, s)$. By summation over s_{n+1}, the equation above gives:

$$0 = s_1 F_1(s_2, \ldots, s_n) - F_1(s_1 s_2, \ldots, s_n) + \cdots + (-1)^n F_1(s_1, \ldots, s_{n-1}) + (-1)^{n+1} m f(s_1, \ldots, s_n).$$

[To compute the one before last term on the right, we have used the fact that, if s_{n+1} runs through G, so does $s_n s_{n+1}$.] Thus we obtain

$$0 = dF_1(s_1, \ldots, s_n) - (-1)^n m f(s_1, \ldots, s_n).$$

Therefore, $mf = d((-1)^n F_1)$.

Corollary 4.4. *If the map : $a \mapsto ma$ is an automorphism of A, then $H^n(G, A) = 0$ for all $n \geqslant 1$.*

Proof. Indeed, $x \mapsto mx$ is an automorphism of $C^n(G, A)$ that commutes with d. Therefore, we obtain an automorphism of $H^n(G, A)$ by passing to the quotient. But the map is zero; hence, $H^n(G, A) = 0$.

Corollary 4.5. *If A is finite of order prime to m, then $H^n(G, A) = 0$ for all $n \geqslant 1$.*

Proof. This follows from cor.4.4.

Corollary 4.6. *If A is finitely generated, then $H^n(G, A)$ is finite for all $n \geqslant 1$.*

Proof. The cochain groups $C^n(G, A)$ are finitely generated, hence the same is true for the $H^n(G, A)$. For $n > 0$, we have $m.H^n(G, A) = 0$; hence, the $H^n(G, A)$ are finitely generated $\mathbf{Z}/m\mathbf{Z}$-modules; this implies that they are finite.

Remark. There is a generalization of th.4.3 where one does not assume that G is finite:

Let G' be a subgroup of G of finite index m; every cochain of G defines by restriction to G' a cochain of G'; one thus obtain a **restriction map** $\mathrm{Res} : H^n(G, A) \to H^n(G', A)$. Then, **if $x \in H^n(G, A)$ is such that $\mathrm{Res}(x) = 0$, then $mx = 0$.**

The proof uses the **corestriction map** $\mathrm{Cor} : H^n(G', A) \to H^n(G, A)$ and the fact that $\mathrm{Cor}(\mathrm{Res}(x)) = mx$, see e.g. Brown [11], III.9, or Lang [30], chap.II, prop.1.10. This is especially useful when G is finite and G' is a p-Sylow subgroup of G, since it implies that $\mathrm{Res} : H^n(G, A) \to H^n(G', A)$ is injective if $p^r A = 0$ for some r.

4.3 Extensions, sections and semidirect products

We first define what an extension of two groups is:

Definition 4.4. *Let A and G be two groups. An* ***extension*** *of G by A is a group E, together with an exact sequence :* $1 \to A \to E \to G \to 1$.
[Warning: In the literature, this is often called " an extension of A by G " .]

An extension E' of G by A is said to be **isomorphic** to E if there exists an isomorphism $\varphi : E \to E'$ such that the following diagram is commutative:

$$\begin{array}{ccccccccc} 1 & \to & A & \to & E & \to & G & \to & 1 \\ & & \text{id}\downarrow & & \varphi\downarrow & & \text{id}\downarrow & & \\ 1 & \to & A & \to & E' & \to & G & \to & 1. \end{array}$$

If $1 \to A \to E \to G \to 1$ is an extension of G by A, a **section** of E is a map $h : G \to E$, such that the composite map $G \to E \to G$ is the identity. If π denotes the projection $E \to G$, this means that $\pi \circ h = \text{id}_G$.

A section h which is a group homomorphism is called a **splitting** of E; if such a section exists, we say that E **splits**. If h is a splitting, its image is a subgroup C of E, with $C \cap A = 1$ and $A.C = E$; the projection $E \to G$ gives an isomorphism $C \to G$, and C is called a **lifting of** G **in** E. If we identify C with G, then every element of E can be written uniquely as ax with $a \in A$ and $x \in G$; the group E is said to be the **semidirect product** of G and A; the composition law of E is $ax.by = a.xbx^{-1}.xy$; it only depends on A, G, and the action of G on A.

Conversely, if a group G acts by automorphisms $a \mapsto {}^x a$ on a group A, the semidirect product of G and A is the group E (denoted by $A \rtimes G$, or simply by $A.G$) made up of the pairs (a, x) with $a \in A$ and $x \in G$, equipped with the group law

$$(a, x)(b, y) = (a\,{}^x b, xy).$$

4.4 Extensions with abelian kernel

Let E be an extension of G by A. We assume in this section that A **is abelian**.

Under this assumption, the natural homomorphism $E \to \text{Aut}(A)$ given by the int_z, $z \in E$, is trivial on A, hence gives a homomorphism $G \to \text{Aut}(A)$, i.e., *an action of G on A*; that action makes A into a G-module. Since we are using a multiplicative notation, the G-action on A will be written below as $a \mapsto {}^x a$ for $a \in A$ and $x \in G$.

[Note that this action is trivial when A is contained in the center of E; one then says that E is a *central extension* of G.]

Let us now start with a given action of G on A. We are going to see (cf. th.4.11) that *the isomorphism classes of extensions of G by the G-module A are in one-one*

correspondence with the elements of $H^2(G, A)$.
More precisely:

Let E be an extension of G by A, and let $\pi : E \to G$ be the projection of E onto G. Choose a section $h : G \to E$; we have $\pi(h(x)) = x$ if $x \in G$. Every element $e \in E$ can be written uniquely as $ah(x)$, with $a \in A$ and $x = \pi(e) \in G$. Let $bh(y)$ be another element of E. We have

$$ah(x)bh(y) = ah(x)bh(x)^{-1}h(x)h(y).$$

The action of $x \in G$ on A is given by conjugation by any lifting of x in E, for instance $h(x)$. Therefore, $h(x)bh(x)^{-1} = {}^x b$. Define now $f_h : G \times G \to A$ by:

$$h(x)h(y) = f_h(x, y)h(xy). \tag{4.4}$$

We have :

$$ah(x)bh(y) = (a\, {}^x b f_h(x, y))\, h(xy) \quad \text{with} \quad a\, {}^x b f_h(x, y) \in A. \tag{4.5}$$

Proposition 4.7. *The map f_h is a 2-cocycle on G with values in A.*

Proof. Let us check that $df_h = 0$. In multiplicative notation, this means $df_h(x, y, z) = 1$ for all $x, y, z \in G$. Let us write $h(x)h(y)h(z)$ in two ways:

$$h(x)h(y).h(z) = f_h(x, y)h(xy).h(z) = f_h(x, y)f_h(xy, z)h(xyz),$$

and

$$h(x).h(y)h(z) = h(x).f_h(y, z)h(yz) = {}^x f_h(y, z)f_h(x, yz)h(xyz);$$

hence $f_h(x, y)f_h(xy, z) = {}^x f_h(y, z)f_h(x, yz)$, which is equivalent to $df_h(x, y, z) = 1$.

Proposition 4.8. *If h and h' are two sections of π, the cocycles f_h and $f_{h'}$ are cohomologous. Conversely, every 2-cocycle which is cohomologous to f_h is equal to some $f_{h'}$.*

Proof. For every $x \in G$ we have $h'(x) = \ell(x)h(x)$, where ℓ is a map of G into A. Let us compute $f_{h'}$ in terms of ℓ and f_h. We have

$$h'(x)h'(y) = f_{h'}(x, y)h'(xy) = f_{h'}(x, y)\ell(xy)h(xy); \tag{4.6}$$

on the other hand, we have

$$\begin{aligned} h'(x)h'(y) &= \ell(x)h(x)\ell(y)h(y) \\ &= \ell(x)h(x)\ell(y)h(x)^{-1}h(x)h(y) \\ &= \ell(x)\, {}^x\ell(y)f_h(x, y)h(xy). \end{aligned} \tag{4.7}$$

From (4.6) and (4.7), we obtain

$$\begin{aligned} f_{h'}(x, y) &= \ell(x)\, {}^x\ell(y)f_h(x, y)\ell(xy)^{-1} \\ &= f_h(x, y)\, {}^x\ell(y)\ell(x)\ell(xy)^{-1}, \end{aligned} \tag{4.8}$$

where we used the assumption that A is abelian to obtain (4.8). On the other hand, in multiplicative notation, we have

$$d\ell(x,y) = {}^x\ell(y)\ell(x)\ell(xy)^{-1},$$

hence $f_{h'} = f_h \, d\ell$, which shows that f'_h and f_h are cohomologous. Conversely, if f' is a 2-cocycle of the form $f_h d\ell$, where ℓ is a 1-cochain, we have $f' = f_{h'}$ with $h' = \ell h$.

Let $[E]$ be the image of f_h in $H^2(G,A)$; the proposition above shows that $[E]$ does not depend on the choice of the section h.

Proposition 4.9. *Two extensions E_1 and E_2 of G by A are isomorphic if and only if $[E_1] = [E_2]$ in $H^2(G,A)$.*

Proof. The "only if" direction is clear. Conversely, if $[E_1] = [E_2]$, let us choose two sections h_1 and h_2 of $E_1 \to G$ and $E_2 \to G$; by assumption, the corresponding factor sets f_{h_1} and f_{h_2} are cohomologous; by changing h_2, we may assume that they are equal. In that case, equation (4.5) shows that the bijection $E_1 \to E_2$ defined by $ah_1(x) \mapsto ah_2(x)$ is an isomorphism.

Proposition 4.10. *Every element of $H^2(G,A)$ is equal to $[E]$, for a suitable extension E of G by A.*

Proof. Here it is convenient to write A additively. Let α be an element of $H^2(G,A)$, and let f be a normalized 2-cocycle representing α. Let $E = A \times G$ and define a multiplication law on E by

$$(a,x).(b,y) = (a + xb + f(x,y), xy). \tag{4.9}$$

The set E is a group for that multiplication. Indeed:

- Associativity: The same computation as in the proof of prop.4.7 shows that the composition law of E is associative because $df = 0$.
- Identity element: Formula (4.3) shows that $f(x,1) = f(1,x) = 0$ for every $x \in G$; this implies that $(0,1)$ is an identity element of E.
- Inverse: The inverse of (a,x) is (b,x^{-1}) with $b = -xa - f(x,x^{-1})$. [Note that $f(x,x^{-1}) = f(x^{-1},x)$; this follows from $df(x,x^{-1},1) = 0$.]
- The kernel of $E \to G$ is $A = \{(a,1), a \in A\}$. Hence E is an extension of G by A, and the cocycle corresponding to the section $x \to (0,x)$ is f.

We have thus proved :

Theorem 4.11. *The map $E \mapsto [E]$ gives a bijection :*

isomorphism classes of extensions of G by $A \iff$ elements of $H^2(G,A)$.

Note that, in this bijection, the split extensions correspond to the element 0 of $H^2(G, A)$.

Corollary 4.12. *If G and the G-module A are finite of relatively prime orders, then every extension of G by A splits.*

Proof. Indeed, we have $H^2(G, A) = 0$, cf. cor.4.5.

Interpreting $H^1(G, A)$ in terms of split extensions. Let E be a split extension of G by A. Choose a splitting $h : G \to E$. Let h' be another splitting; we can write h' uniquely as $h' = \ell.h$, where $\ell : G \to A$ is a 1-cochain. We have $f_{h'} = f_h.d\ell = d\ell$ since $f_h = 1$. For h' to be a homomorphism it is necessary and sufficient that $f_{h'} = 1$, i.e., that $d\ell = 1$, i.e., that ℓ is a 1-cocycle. If that cocycle is the coboundary of an element $a \in A$, we have $h'(x) = a\,.\,{}^x a^{-1} h(x) = a$

Moreover, if we conjugate h by an element $a \in A$, we obtain another splitting h_a. The corresponding cocycle ℓ is given by $\ell(x) = a\,.\,{}^x a^{-1}$. Therefore, $\ell = da$. Thus, ℓ is a coboundary. Hence:

Theorem 4.13. *The conjugacy classes (by elements of A or, equivalently, of G) of splittings of E are in bijective correspondence with the elements of the cohomology group $H^1(G, A)$.*

[Note that the correspondence depends on the choice of the splitting h. A more precise statement is that the splittings make up a $Z^1(G, A)$-torsor, and their conjugacy classes make up an $H^1(G, A)$-torsor.]

Corollary 4.14. *The splittings of a split extension are conjugate to each other if and only if $H^1(G, A) = 0$.*

Corollary 4.15. *If G and A are finite of relatively prime orders, and if E is an extension of G by A, then every two splittings of E are conjugate.*

Proof. Indeed, we have $H^1(G, A) = 0$, cf. cor.4.5.

4.5 Extensions with arbitrary kernel

The results of the previous section also hold (with some modifications, see below) when the kernel A of the extension is nonabelian. The cohomology groups which occur are the $H^n(G, Z(A))$ for $n = 1, 2, 3$, where $Z(A)$ is the center of A. This is due to Eilenberg-Mac Lane [50]. We shall only sketch the proofs: they rely on computations similar to those of the previous section and their details can be found in [50] and in Morandi [69]. Note also that the case where G is cyclic can be done by direct constructions, cf. exerc.11.

4.5.1. The homomorphisms $E \to \mathrm{Aut}(A)$, $G \to \mathrm{Out}(A)$ and $G \to \mathrm{Aut}(Z(A))$.

Let $1 \to A \to E \to G \to 1$ be an extension. The group E acts on A by

$$E \to \mathrm{Int}(E) \to \mathrm{Aut}(A).$$

This gives a homomorphism $\psi_E : E \to \mathrm{Aut}(A)$ which maps A into $\mathrm{Int}(A)$, hence gives a homomorphism

$$\psi : G \to \mathrm{Out}(A).$$

The natural homomorphism $\mathrm{Aut}(A) \to \mathrm{Aut}(Z(A))$ is trivial on $\mathrm{Int}(A)$, hence defines $\mathrm{Out}(A) \to \mathrm{Aut}(Z(A))$; by composition with ψ, this gives $\psi_0 : G \to \mathrm{Aut}(Z(A))$, which makes $Z(A)$ into a G-module. [When A is abelian, we have $Z(A) = A$, and we recover the situation of the previous section.] In what follows, *we select a homomorphism* $\psi : G \to \mathrm{Out}(A)$, hence also $\psi_0 : G \to \mathrm{Aut}(Z(A))$, and we look at the corresponding extensions.

4.5.2. The existence problem and its obstruction in $H^3(G, Z(A))$.

The first question is whether, for a given ψ, there exists an extension E of G by A corresponding to ψ. When A is abelian, the answer is "yes" : just take for E the semidirect product of G by A. Such a construction is not possible in general, because the map $\psi : G \to \mathrm{Out}(G)$ does not always lift to $G \to \mathrm{Aut}(G)$. Indeed, there are cases where no extension exists: see exerc.12 for an example with $|G| = 2$ and $|A| = 16$. What Eilenberg and Mac Lane did is to *associate to ψ an element $c(\psi)$ of $H^3(G, Z(A))$* and to prove :

Theorem 4.16. *There exists an extension of G by A corresponding to ψ is and only if $c(\psi) = 0$.*

The construction of $c(\psi)$ is as follows: select a map $s : G \to \mathrm{Aut}(A)$ such that the composite map $G \xrightarrow{s} \mathrm{Aut}(A) \to \mathrm{Out}(A)$ is ψ. For every $x, y \in G$, choose $\varphi(x, y) \in A$ such that $\mathrm{int}_{\varphi(x,y)} = s(x)s(y)s(xy)^{-1}$, and put :

$$c(x, y, z) = {}^{s(x)}\varphi(y, z)\varphi(x, yz)\varphi(xy, z)^{-1}\varphi(x, y)^{-1} \quad \text{for} \quad x, y, z \in G.$$

[Here, the term ${}^{s(x)}\varphi(y, z)$ means the transform of $\varphi(y, z)$ by the automorphism $s(x)$.] A simple computation shows that $\mathrm{int}_{c(x,y,z)} = 1$, i.e., that $c(x, y, z)$ belongs to $Z(A)$; one also checks that it is a 3-cocycle and that its class in $H^3(G, Z(A))$ is independent of the choices of s and f; that class is $c(\psi)$. Another simple computation shows that $c(\psi) = 0$ if there exists an extension of G by A corresponding to ψ. The converse is true; for the proof, see [50] or [69].

4.5.3. Classification of the extensions of G by A.

The next question is:

Suppose that there exists an extension E corresponding to ψ. What are the other ones ?

Answer (cf. [50]) : *they correspond to the elements of $H^2(G, Z(A))$.*

To state the result more precisely, denote by $\mathrm{Ext}(G, A, \psi)$ the isomorphism classes of extensions of G by A corresponding to ψ. Let us define an action of the group $H^2(G, Z(A))$ on the set $\mathrm{Ext}(G, A, \psi)$:

Let E be an extension and let F be an element of $H^2(G, Z(A))$. Choose a normalized 2-cocycle f in the class F. Let E_f be the set E endowed with the multiplication law:

$$e \bullet_f e' = f(x, x')ee', \tag{4.10}$$

where x and x' are the images of e and e' in G. A computation shows that E_f is a group, which contains A as a normal subgroup with $E_f/A \simeq G$, and $\psi_{E_f} = \psi_E$; moreover, the isomorphism class of the extension E_f does not depend on the choice of f. Hence the class $E \bullet F$ of E_f in $\mathrm{Ext}(G, A, \psi)$ is well defined. We have $E \bullet (F + F') \simeq (E \bullet F) \bullet F'$: this gives the action we wanted to define.

[For a cocycle-free construction of $E \bullet F$, see exerc.9.]

Theorem 4.17. *The action of $H^2(G, Z(A))$ on $\mathrm{Ext}(G, A, \psi)$ is free; it is transitive if $\mathrm{Ext}(G, A, \psi)$ is not empty.*

[In other words: $\mathrm{Ext}(G, A, \psi)$ is, either empty, or an $H^2(G, A)$-torsor.]

Let us prove that the action is free. With the notation above, we have to show that, if $E_f \simeq E$, then f is a coboundary. Let $\varphi : E_f \to E$ be an isomorphism (of extensions). We may write φ as $e \mapsto r(e)e$, where r is a map of E into A. The fact that φ is a homomorphism gives :

$$f(x, x')r(ee')ee' = r(e)er(e')e' \quad \text{for every} \quad e, e' \in E, \tag{4.11}$$

where x, x' are the images of e, e' in G.

Let us apply equation (4.11) with $e' \in A$; since φ is the identity on A, and f is normalized, it shows that $r(ea) = r(e)$ for every $e \in E$ and $a \in A$; hence r may be viewed as a function $x \mapsto r(x)$ on G. Applying (4.11) with $e \in A$ shows that $ar(x) = r(x)a$ for every $a \in A$, i.e., that $r(x)$ belongs to $Z(A)$. Hence r is a 1-cochain on G with values in $Z(A)$. We may then rewrite (4.11) as :

$$f(x, x')r(xx')ee' = r(x).er(x')e^{-1}.ee', \quad \text{i.e.,} \quad f(x, x')r(xx') = r(x).{}^x r(x'),$$

which means that f is the coboundary of r, as wanted.

For a proof of the transitivity of the action, see exerc.10.

Corollary 4.18. *If G and $Z(A)$ are finite, so is $\mathrm{Ext}(G, A, \psi)$, and its cardinality is either 0 or the order of $H^2(G, Z(A))$.*

Corollary 4.19. *If $H^2(G, Z(A))$ and $H^3(G, Z(A))$ are both 0, then $|\mathrm{Ext}(G, A, \psi)| = 1$.*

Remark. When $Z(A) = 1$, these corollaries show that there is only one extension (up to isomorphism) corresponding to a given $\psi : G \to \mathrm{Out}(A)$. This is easy to see directly; indeed E is isomorphic to the subgroup of $G \times \mathrm{Aut}(A)$ made up of the pairs of elements which have the same image in $\mathrm{Out}(A)$.

4.6 Extensions of groups of relatively prime orders

The following result generalizes cor.4.12 and cor.4.15 to extensions with an arbitrary kernel :

Theorem 4.20 (Zassenhaus). *Let $1 \to A \to E \to G \to 1$ be an extension, where A and G are two finite groups of relatively prime orders. Then :*

(1) *The extension E splits.*
(2) *If A or G is solvable, two different splittings of E are conjugate by an element of A.*

Proof. Use induction on $|E|$. We may assume that A and G are nontrivial.

Proofs of (1) *and* (2) *when A is solvable.*

Let A' be an abelian nontrivial characteristic subgroup A' of A; such a subgroup exists, cf. cor.3.3. Note that A' is normal in E: an inner automorphism of E restricted to A is an automorphism of A and therefore leaves A' invariant. If $A = A'$, then A is abelian and the theorem follows from cor.4.12 and cor.4.15. Otherwise, since A' is normal in E, we have the exact sequence

$$1 \longrightarrow A/A' \longrightarrow E/A' \longrightarrow G \longrightarrow 1 .$$

Since the order of E/A' is strictly less than that of E, the induction hypothesis implies that G lifts to a subgroup G' of E/A'. Let E' be the inverse image of G' under the projection $E \to E/A'$. Therefore, we have the following exact sequence :

$$1 \longrightarrow A' \longrightarrow E' \longrightarrow G' \longrightarrow 1 .$$

Since A' is abelian, cor.4.12 shows that G' can be lifted in E'. Hence G can be lifted in E.

Let us now check that every two such liftings G_1 and G_2 are conjugate by an element in A. We have

$$E = A.G_1 \quad \text{and} \quad E = A.G_2.$$

The induction hypothesis applied to E/A' shows that there exists $a \in A$ such that aG_1a^{-1} and G_2 have the same image in E/A'. After replacing G_1 by aG_1a^{-1}, we may assume that $A'.G_1 = A'.G_2$. By cor.4.15, applied to $A'.G_1 = A'.G_2$, we see that G_1 and G_2 are conjugate in E .

Proof of (1) *in the general case.*

Let p be a prime number dividing the order of A and let S be a p-Sylow subgroup of A. Let E' be the normalizer of S in E. According to prop.2.11 (Frattini), we have $E = A.E'$. The group $A' = E' \cap A$ is normal in E' and we have the exact sequence

$$1 \longrightarrow A' \longrightarrow E' \longrightarrow G \longrightarrow 1\,.$$

There are two cases:

(1) If $|E'| < |E|$, the induction hypothesis allows us to lift G to E', and therefore to E.

(2) If $|E'| = |E|$, then S is normal in E and therefore normal in A. We have the exact sequence :

$$1 \longrightarrow A/S \longrightarrow E/S \longrightarrow G \longrightarrow 1\,.$$

Since $|E/S| < |E|$, the induction hypothesis shows that G lifts to a subgroup G_1 of E/S. Let E_1 be the inverse image of G_1 under the projection $E \to E/S$. We have the exact sequence

$$1 \longrightarrow S \longrightarrow E_1 \longrightarrow G \longrightarrow 1.$$

But S is a p-group; therefore, it is solvable and we know that (1) is valid.

Proof of (2) *when G is solvable.*

Let G_1 and G_2 be two liftings of G in E. We have

$$E = A.G_1 \quad \text{and} \quad E = A.G_2.$$

Let p be a prime number, let I be a nontrivial normal abelian subgroup of G (cf. cor.3.3), and let $\widetilde{I}$ be its inverse image under the projection $E \to G$. Let $I_1 = \widetilde{I} \cap G_1$ and $I_2 = \widetilde{I} \cap G_2$. We have $A.I_1 = \widetilde{I} = A.I_2$. The groups I_1 and I_2 are p-Sylow subgroups of $\widetilde{I}$. Thus, there exists $x \in \widetilde{I}$ such that $I_2 = xI_1x^{-1}$. If we write x in the form ay with $a \in A$ and $y \in I_1$, we have $I_2 = aI_1a^{-1}$. After replacing I_1 by aI_1a^{-1}, we may assume that $I_2 = I_1$.

Let N be the normalizer of $I_1 = I_2$ in E. We have $G_1 \subset N$ and $G_2 \subset N$. If $N \neq E$, the induction hypothesis applied to N shows that G_1 and G_2 are conjugate. If $N = E$, i.e., if I_1 is normal in E, the induction hypothesis applied to E/I_1 shows that there exists $a \in A$ such that $I_1.aG_1a^{-1} = I_1.G_2$. Since I_1 is normal and is contained in both G_1 and G_2, this implies $aG_1a^{-1} = G_2$. This completes the proof.

Remark. The hypothesis "A or G is solvable" for (2) is always satisfied, thanks to the Feit-Thompson theorem (cf. §3.2), which says that a group of odd order is solvable. Indeed, if two integers are relatively prime, one of them is odd !

Corollary 4.21. *Let S be a p-Sylow subgroup of a group G , and let $N = N_G(S)$. The extension $1 \to S \to N \to N/S \to 1$ splits.*

Proof. This follows from the fact that $|S|$ and $|N/S|$ are relatively prime.

Corollary 4.22. *Let $\varphi : G \to G'$ be a surjective homomorphism of finite groups. There exists a subgroup G_1 of G such that $\varphi(G_1) = G'$ and such that the prime divisors of $|G_1|$ and of $|G'|$ are the same.*

Proof. Use induction on $|G|$. It is enough to show that, if a prime number p does not divide $|G'|$, there is a subgroup H of G, of order prime to p, such that $\varphi(H) = G'$. Let S be a p-Sylow of G, and let N be its normalizer. Since S is contained in $\mathrm{Ker}(\varphi)$, the Frattini argument (prop.2.11) shows that $\varphi(N) = G'$. By cor.4.21, there exists a subgroup H of N, of order prime to p, such that $N = SH$. Since $\varphi(N) = G'$ and $\varphi(S) = 1$, we have $\varphi(H) = G'$, as wanted.

4.7 Liftings of homomorphisms

Let $1 \to A \to E \xrightarrow{\pi} \Phi \to 1$ be an exact sequence, let G be a group, and let $\varphi : G \to \Phi$ be a homomorphism. Can we lift φ to a homomorphism of G into E, i.e., can we find $\psi : G \to E$ such that $\pi \circ \psi = \varphi$:

$$\begin{array}{ccccccccc} & & & & G & & & & \\ & & & \psi \swarrow & \downarrow \varphi & & & & \\ 1 & \longrightarrow & A & \longrightarrow E & \longrightarrow & \Phi & \longrightarrow & 1\,? & \end{array}$$

To answer that question, let us introduce the **pull-back** E_φ of E by φ. It is an extension of G by A fitting into a commutative diagram:

$$\begin{array}{ccccccccc} 1 & \to & A & \to & E_\varphi & \to & G & \to & 1 \\ & & \mathrm{id}\downarrow & & \downarrow & & \varphi\downarrow & & \\ 1 & \to & A & \to & E & \to & \Phi & \to & 1. \end{array}$$

Equivalently, E_φ is the subgroup of $E \times G$ made up of the $(e, g) \in E \times G$ such that $\pi(e) = \varphi(g)$; i.e., it is the " product over Φ " of E and G, often denoted by $E \times_\Phi G$.

Proposition 4.23. *The liftings of φ are in one-one correspondence with the splittings of E_φ.*

Proof. This is clear on the set-theoretic level: a map $\psi : G \to E$ such that $\pi \circ \psi = \varphi$ corresponds to a map $\psi_0 : G \to E_\varphi$ such that the composite $G \to E_\varphi \to G$ is the identity. Moreover, ψ is a homomorphism if and only if ψ_0 is a homomorphism.

Note also that two liftings ψ' and ψ'' are conjugate by $a \in A$ if and only if $G_{\psi'}$ and $G_{\psi''}$ are conjugate by $(a, 1) \in E_\varphi$. Theorem 4.20 then gives:

Theorem 4.24. *Let $1 \to A \to E \to \Phi \to 1$ be an exact sequence and let $\varphi : G \to \Phi$ be a homomorphism. Suppose that G and A are finite groups of relatively prime orders. Then :*

(1) *There exists a homomorphism $\psi : G \to E$ lifting φ.*

(2) *If G or A is solvable, two such homomorphisms are conjugate by an element of A.*

4.8 Application to p-adic liftings

4.8.1. The p-adic numbers.

Let us recall a few definitions (see Lang [29], chap.I, §10 and chap.XII, §6, or [36], chap.II). If p is a prime number, we have natural ring homomorphisms

$$\cdots \to \mathbf{Z}/p^n\mathbf{Z} \to \mathbf{Z}/p^{n-1}\mathbf{Z} \to \cdots \to \mathbf{Z}/p\mathbf{Z}.$$

A **p-adic integer** is a family $x = (x_n)$, with $x_n \in \mathbf{Z}/p^n\mathbf{Z}$, such that the image of x_n in $\mathbf{Z}/p^{n-1}\mathbf{Z}$ is x_{n-1} for every $n > 1$. The set of p-adic integers is denoted by $\mathbf{Z}_p$. The process we have used to define it is called a *projective limit* or an *inverse limit*, and one writes accordingly:

$$\mathbf{Z}_p = \operatorname{proj\,lim}\ \mathbf{Z}/p^n\mathbf{Z} \quad \text{or} \quad \mathbf{Z}_p = \varprojlim\ \mathbf{Z}/p^n\mathbf{Z}.$$

The set $\mathbf{Z}_p$ is a commutative ring for the composition laws:

$$(x_n) + (y_n) = (x_n + y_n) \quad \text{and} \quad (x_n).(y_n) = (x_n.y_n).$$

It has the following properties, which are easy to check:

(i) It is a domain, i.e., $xy = 0$ implies $x = 0$ or $y = 0$.

(ii) The homomorphism $\mathbf{Z}_p \to \mathbf{Z}/p^n\mathbf{Z}$ is surjective; its kernel is the ideal $p^n\mathbf{Z}_p$.

(iii) An element $x = (x_n)$ of $\mathbf{Z}_p$ is invertible if and only if it does not belong to $p\mathbf{Z}_p$, i.e., if $x_1 \neq 0$.

The field of fractions of $\mathbf{Z}_p$ is the ring $\mathbf{Z}_p[1/p]$ obtained by adjoining $1/p$ to $\mathbf{Z}_p$; it is a field of characteristic zero, which is denoted by $\mathbf{Q}_p$, and is called the **p-adic field**; its elements are the **p-adic numbers**. Every nonzero p-adic number x can be written uniquely as $x = p^m.u$, with $m \in \mathbf{Z}$ and $u \in \mathbf{Z}_p^\times$; the integer m is called the **p-adic valuation** of x, and is denoted by $v_p(x)$.

4.8.2. Lifting a group representation from characteristic p to characteristic 0.

Theorem 4.25. *Let G be a finite group of order prime to p, and let $\rho : G \to \mathrm{GL}_N(\mathbf{F}_p)$ be a homomorphism. There exists a homomorphism $\rho_0 : G \to \mathrm{GL}_N(\mathbf{Z}_p)$ which lifts ρ.*

Proof. Let us first show that $\rho_1 = \rho$ can be lifted to $\rho_2 : G \to \mathrm{GL}_N(\mathbf{Z}/p^2\mathbf{Z})$. We have the exact sequence

$$1 \to A \to \mathrm{GL}_N(\mathbf{Z}/p^2\mathbf{Z}) \to \mathrm{GL}_N(\mathbf{Z}/p\mathbf{Z}) \to 1,$$

where A is the set of matrices of the form $1 + pX$ where X is an $n \times n$ matrix with entries in $\mathbf{Z}/p\mathbf{Z}$ and the map $\mathbf{GL}_N(\mathbf{Z}/p^2\mathbf{Z}) \to \mathbf{GL}_N(\mathbf{Z}/p\mathbf{Z})$ is reduction modulo p. The group A is isomorphic to the additive matrix group $\mathrm{M}_N(\mathbf{Z}/p\mathbf{Z})$, which is an elementary abelian p-group. We can therefore apply th.4.7 to lift ρ_1 to ρ_2.

By the same argument, we can lift ρ_2 to $\rho_3 : G \to \mathrm{GL}_N(\mathbf{Z}/p^3\mathbf{Z})$, etc. The homomorphisms $(\rho_1, \rho_2, \rho_3, \dots)$ give a homomorphism ρ_0 of G into the projective limit of the $\mathrm{GL}_N(\mathbf{Z}/p^m\mathbf{Z})$, which is isomorphic to $\mathrm{GL}_N(\mathbf{Z}_p)$.

Remark. Since $\mathrm{GL}_N(\mathbf{Z}_p)$ is a subgroup of $\mathrm{GL}_N(\mathbf{Q}_p)$, we may view ρ_0 as a linear representation of G over the field $\mathbf{Q}_p$, which is of characteristic 0. This is typical of the way p-adic numbers are used: as a bridge between characteristic p and characteristic 0.

4.9 Exercises

1. (*Homogeneous cochains and the formula $d \circ d = 0$.*) Let G be a group and let A be a G-module. If $n \geqslant 0$, define $C^n_{\mathrm{hom}}(G, A)$ as the group of functions $F : G^{n+1} \to A$ such that

   $F(ss_0, ss_1, \dots, ss_n) = sF(s_0, s_1, \dots, s_n)$ for every $s, s_0, \dots, s_n \in G$.

   a) If F is such a function, define $f \in C^n(G, A)$ by

   $$f(s_1, \dots, s_n) = F(1, s_1, s_1s_2, \dots, s_1 \cdots s_n).$$

   Show that $F \mapsto f$ is an isomorphism $\varepsilon : C^n_{\mathrm{hom}}(G, A) \to C^n(G, A)$, and that its inverse is $f \mapsto F$, where $F(s_0, \dots, s_n) = s_0 f(s_0^{-1}s_1, s_1^{-1}s_2, \dots, s_{n-1}^{-1}s_n)$.

   b) If $F \in C^n_{\mathrm{hom}}(G, A)$ and $0 \leqslant i \leqslant n+1$, define $\partial_i F \in C^{n+1}_{\mathrm{hom}}(G, A)$ by:

   $\partial_0 F(s_0, \dots, s_{n+1}) = F(s_1, \dots, s_{n+1})$,

   and

   $\partial_i F(s_0, \dots, s_{n+1}) = F(s_0, \dots, s_{i-1}, s_{i+1}, \dots, s_{n+1})$, for $i > 0$.

   Define $\partial F = \sum_{i=0}^{n+1} (-1)^i \partial_i F$. Show that $\partial_i \partial_j F = \partial_{j-1} \partial_i F$ if $i < j$, hence $\partial\partial F = 0$.
   c) Show that the isomorphism $\varepsilon : C^n_{\mathrm{hom}}(G, A) \to C^n(G, A)$ is such that $\varepsilon \circ \partial = d \circ \varepsilon$, and conclude that $d \circ d = 0$.

2. (*Interchanging x and y in a 2-cocycle.*) Let $f \in Z^2(G, A)$ be a 2-cocycle. Define f' in $C^2(G, A)$ by $f'(x, y) = -xyf(y^{-1}, x^{-1})$. Show that f' is a 2-cocycle cohomologous to f. [Hint: choose an extension E of G by A and a section $h : G \to E$ such that

   $$h(x)h(y) = f(x, y)h(xy);$$

   define a section h' by $h'(x) = h(x^{-1})^{-1}$; show that $h'(x)h'(y) = f'(x, y)h'(xy)$; this implies that f and f' are cohomologous.]

3. (1- *and* 2-*cocycles for cyclic groups*) Let G be a cyclic group of finite order n, with generator σ, and let A be a G-module. Let T and D be the endomorphisms of A defined by : $T = \sum_{g \in G} g = 1 + \sigma + \cdots + \sigma^{n-1}$ and $D(x) = \sigma - 1$.
   a) Let $a \in A$ be such that $T(a) = 0$. Let $f_a : G \to A$ be the map:

   $$\sigma^i \mapsto (1 + \sigma + \cdots + \sigma^{i-1})a \ \text{ for } \ 0 \leqslant i < n.$$

   Show that f_a is a 1-cocycle, and that every 1-cocycle is equal to some f_a; show that f_a is a coboundary if and only if $a = D(b)$ for some $b \in A$. Hence $H^1(G, A) \simeq \mathrm{Ker}(T)/\mathrm{Im}(D)$.

b) Let $a \in A$ be fixed under the action of G, i.e., $D(a) = 0$. Let $F_a : G \times G \to A$ be the map defined by:

$$F_a(\sigma^i, \sigma^j) = \begin{cases} 0 & \text{if } 0 \leqslant i,j < n, \quad i+j < n, \\ a & \text{if } 0 \leqslant i,j < n, \quad i+j \geqslant n. \end{cases}$$

Show that F_a is a 2-cocycle, and that every 2-cocycle is cohomologous to some F_a, where a is well defined modulo $\mathrm{Im}(T)$. Hence $H^2(G, A) \simeq \mathrm{Ker}(D)/\mathrm{Im}(T) = A^G/TA$.
[Hint: use the interpretation of $H^2(G, A)$ as classes of extensions of G by A.]

4. (*A splitting criterion for some extensions of a dihedral group.*)
Let $1 \to A \to E \to \mathcal{D}_n \to 1$ be an extension of a dihedral group $\mathcal{D}_n$ of order $2n, n > 0$, by a group A of order 2. Suppose that every element of order 2 of $\mathcal{D}_n$ is the image of an element of order 2 of E. Show that the extension E splits.
[Hint: let x, y be two elements of E of order 2 whose images x', y' in $\mathcal{D}_n$ have order 2 and generate that group; let $z = xy$; the image z' of z in $\mathcal{D}_n$ has order n. There are two cases:
(i) n is even. In that case, z has order n: if not, it would have order $2n$ and $z^{n/4}$ would be an element of E of order 4 whose image in $\mathcal{D}$ would be of order 2. Hence x, y generate a subgroup of order $2n$ of E, which is a lifting of $\mathcal{D}_n$: the extension E splits.
(ii) n is odd. If z has order n, the same agument as in (i) shows that E splits. If z has order $2n$, then $a = z^n$ is the nontrivial element of A. The elements ax, y have the same image in $\mathcal{D}_n$ than x, y, and they have order 2. Moreover $(axy)^n = a^n(xy)^n = az^n = 1$. Hence ax, y generate a subgroup of E isomorphic to $\mathcal{D}_n$, and the argument of (i) applies.]

[For an application to the extensions of $\mathcal{A}_4, \mathcal{A}_5$ and $\mathcal{A}_6$ by a group of order 2, see chap.10, exerc.3.]

5. (*The Nakayama map.*) Let G be a finite group acting on an abelian group A; denote by T the endomorphism $a \mapsto \sum_{g \in G} ga$; we have $TA \subset A^G$.
Let $f \in Z^2(G, A)$ be a 2-cocycle. Define $Sf : G \to A$ by : $Sf(x) = \sum_{z \in G} f(z, x)$.
a) Show that $Sf(x) \in A^G$.
[Hint: use $df(z, t, x) = 0$ to show that $zSf(x) = f(x)$ for every $z \in G$.]
b) Suppose that $f = dF$, where F is a map $G \to A$. Show that $Sf(x) = T(F(x))$.
c) If $x \in G$, let $Nf(x) \in A^G/TA$ be the image of $Sf(x)$ in A^G/TA.
Show that $Nf : G \to A^G/TA$ is a homomorphism.
[Hint : show that $Sf(xy) = Sf(x) + Sf(y)) - T(f(x, y))$.]
d) Deduce from a), b), c) that N is a homomorphism : $H^2(G, A) \to \mathrm{Hom}(G, A^G/TA)$; that endomorphism is called the *Nakayama map.*
[For an interpretation of that map in terms of transfer, see chap.7, exerc.12, and Lang [30], chap.VIII.2.]
e) Suppose that G is cyclic with generator σ. Identify $\mathrm{Hom}(G, A^G/TA)$ with A^G/TA by $\varphi \mapsto \varphi(\sigma)$; identify $H^2(G, A)$ with A^G/TA as in exerc.3. Show that these identifications transform the Nakayama map into the identity map $A^G/TA \to A^G/TA$.

6. (*p-groups such that every subgroup of order p^2 is cyclic.*)
Let p be a prime number $\neq 2$.
a) Let C be a cyclic group of order p, and let A be a cyclic group of order $p^n, n > 0$. Show that every extension E of C by A is either cyclic, isomorphic to $C \times A$ or (if $n > 1$)

a semidirect product of C by A relatively to a nontrivial action of C on A.
[Hint: use exerc.3 to show that $H^2(C, A)$ is cyclic of order p if the action of C on A is trivial, and is 0 if not.]
Deduce that, either E is cyclic, or it contains a subgroup isomorphic to $C \times C$.
b) Let G be a p-group which does not contain any subgroup isomorphic to $C \times C$. Show that G is cyclic.
[Hint: Let A be a normal cyclic subgroup of G of maximal order. Suppose that $H \neq G$. Choose a central subgroup C of G/A of order p and let E be its inverse image in G. By a), E is cyclic; this contradicts the maximality property of A. Hence $G = A$.]

7. (*Central extensions by* $\mathbf{Z}$.)
Let G be a finite group, n an integer $\geqslant 1$, and $\chi : G \to \mathbf{Z}/n\mathbf{Z}$ a homomorphism. Let G_χ be the subgroup of $G \times \mathbf{Z}$ made up of the pairs (g, z) such that $\chi(g) \equiv z \pmod{n}$. We have an exact sequence:
$$1 \to \mathbf{Z} \to G_\chi \to G \to 1,$$
where the map $\mathbf{Z} \to G_\chi$ is $z \mapsto (1, z)$ and the map $G_\chi \to G$ is $(g, z) \mapsto g$. Hence G_χ is a central extension of G by $\mathbf{Z}$.
a) Show that the elements of finite order of G_χ are the pairs (g, z) such that $\chi(g) = 0$. Show that, if there is no such element $\neq 1$, then χ is injective, G is cyclic and $G_\chi \simeq \mathbf{Z}$.
b) Assume that n is a multiple of $|G|$. Show that every central extension of G by $\mathbf{Z}$ is isomorphic to some G_χ.
[Hint: Let E be such an extension, and $f : G \times G \to \mathbf{Z}$ be a corresponding 2-cocycle. By th.4.3, there exists $F : G \to \mathbf{Z}$ such that $nf = d(F)$. By reduction mod n, the map F defines a map $\chi : G \to \mathbf{Z}/n\mathbf{Z}$. Show that χ is a homomorphism and that $E \simeq G_\chi$.]

8. (*Interpretation of* $H^1(G, Z(A))$ *in terms of automorphisms.*) Let $1 \to A \to E \to G \to 1$ be an extension. The group G acts in a natural way on $Z(A)$. Let $f : G \to Z(A)$ be a 1-cocycle relative to this action. Let $\varphi_f : E \to E$ be the map $x \mapsto f(x_G)x$, where x_G is the image of x in G.
a) Show that φ_f is an automorphism of E which acts trivially on A and on $G = E/A$.
b) Show that every automorphism of E having these properties is equal to φ_f for a suitable f. Show that the class of f in $H^1(G, Z(A))$ is 0 if and only if $\varphi_f = \mathrm{int}_z$ for some $z \in Z(A)$.

9. (*Alternative definition of the action of* $H^2(G, A)$ *on* $\mathrm{Ext}(G, A, \psi)$.)
Keep the notation of §4.5. Let E (resp. F) be an extension of G by A (resp. by $Z(A)$) corresponding to ψ (resp. to ψ_0). Let Δ_G be the diagonal of $G \times G$, and let $E \times_G F$ be the inverse image of Δ_G under the map $E \times F \to G \times G$. We have an exact sequence:
$$1 \to A \times Z(A) \to E \times_G F \to G \to 1.$$
Let Δ^- be the subgroup of $A \times Z(A)$ made up of the pairs (a, z) with $az = 1$. It is a normal subgroup of $E \times_G F$. The quotient $(A \times Z(A))/\Delta^-$ can be identified with A, via the map $a \mapsto (a, 1)$. Let $E \bullet F = (E \times_G F)/\Delta^-$. We have an exact sequence:
$$1 \to A \to E \bullet F \to G \to 1.$$
Show that this extension of G by A is isomorphic to that defined by the cocycle construction of §4.5.

10. (*Transitivity of the action of* $H^2(G,A)$ *on* $\mathrm{Ext}(G,A,\psi)$.)
Keep the notation of §4.5 and exerc.9. Let E and E' be two extensions of G by A corresponding to ψ. Let Γ be the subgroup of $E \times_G E'$ made up of the pairs (e,e') such that $\psi_E(e) = \psi_{E'}(e')$.
a) Show that the map $\Gamma \to G$ is surjective and that its kernel B is the subgroup of $A \times A$ made up of the pairs (a,a') such that $a \equiv a' \bmod Z(A)$.
b) Let Δ be the diagonal of $A \times A$. Show that it is a normal subgroup of Γ. The quotient B/Δ may be identified with $Z(A)$ via the map $(a,a') \mapsto a^{-1}a'$. Let $F = \Gamma/\Delta$. Show the exactness of $1 \to Z(A) \to F \to G \to 1$.
c) Show that $E \bullet F \simeq E'$.
[Hint: Define a map $E \times_G F \to E'$ by $(e_1,(e,e')) \mapsto e_1e^{-1}.e'$; note that this makes sense, since e_1e^{-1} belongs to A, hence can be multiplied with any element of E'. Show that this map is a homomorphism, and that its kernel is the same as the kernel of $E \times_G F \to E \bullet F$. Hence $E \bullet F$ and E' are isomorphic.]

11. (*Extensions of a finite cyclic group.*) Keep the notation of §4.5 and suppose that G is cyclic of finite order n, with generator s. If $\psi : G \to \mathrm{Out}(A)$ is a homomorphism, there exists a representative σ of $\psi(c)$ in $\mathrm{Aut}(A)$ and an element $a \in A$ such that $\sigma^n = \mathrm{int}_x$. To such a pair (σ, x) we associate the element $c = \sigma(x)x^{-1}$ of A.
a) Show that c belongs to $Z(A)$.
b) Let D and T be the endomorphisms of $Z(A)$ defined as in exerc.3, namely:
$$D(z) = \sigma(z)z^{-1} \quad \text{and} \quad T(z) = z.\sigma(z)\cdots\sigma^{n-1}(z).$$
[Note that the restriction of σ to $Z(A)$ is $\psi_0(s)$; it does not depend on the choice of σ.]
Let $Z(A)_T$ be the kernel of T and $Z(A)^D$ be the image of D. Show that c belongs to $Z(A)_T$ and that its class $c(\psi)$ in $Z(A)_D/Z(A)^T$ is independent of the choice of (σ,x); it only depends on ψ.
c) Show that $c(\psi) = 1$ if there exists an extension E of G by A corresponding to ψ.
[Hint: choose $e \in E$ with image s in G; put $\sigma = \psi_E(e)$ and $x = e^n$; then $c = 1$.]
d) Conversely, if $c(\psi) = 1$, show that there exists an extension E of G by ψ corresponding to ψ.
[Hint: show first that σ and x can be chosen such that $c = 1$. In that case, let L be a group isomorphic to $\mathbf{Z}$ with generator ℓ and let $A.L$ be the semidirect product of L and A, with ℓ acting on A by σ. Let N be the subgroup of $A.L$ generated by the element $x^{-1}\ell^n$. Show that N is contained in the center of $A.L$ and that the quotient $E = (A.L)/N$ is an extension of G by A corresponding to ψ.]

12. (*An example of* $\psi : G \to \mathrm{Out}(A)$ *for which no extension exists.*) Let A be the generalized quaternion group of order 16; it is generated by two elements x and y, of order 8 and 4, such that $y^2 = x^4$ and $yxy^{-1} = x^{-1}$; its center is $\{1, x^4\}$.
(a) Let σ be the automorphism of A such that $\sigma(x) = x^5$ and $\sigma(y) = yx^2 = x^{-2}y$. Show that $\sigma^2 = \mathrm{int}_{x^{-1}}$ and that $\sigma(x^{-1}) = x^{-1}.x^4$.
(b) Let $G = \{1, s\}$ be a group of order 2. Let $\psi : G \to \mathrm{Out}(A)$ be such that $\psi(s)$ is the image of σ in $\mathrm{Out}(A)$. Apply exerc.11 with $n = 2$; the group $Z(A)_D$ is equal to $\{1, x^4\}$ and $Z(A)^T = 1$; the invariant $c = c(\psi)$ is equal to x^4, hence is nontrivial, and this shows that there is no extension of G by A corresponding to ψ.
(c) Show that this example is minimal in the following sense: if G and A are finite groups such that $|A|.|G| < 32$, every homomorphism $G \to \mathrm{Out}(A)$ corresponds to an extension of G by A.

[Hint: check that the extension $1 \to \mathrm{Int}(A) \to \mathrm{Aut}(A) \to \mathrm{Out}(A) \to 1$ splits if $|A| < 16$ and $Z(A) \neq 1$.]

13. (*Non emptiness of a projective limit of finite sets.*) Let $\cdots \to X_n \to \cdots \to X_1$ be a family of maps between finite sets.
a) If $m \geqslant n$, let $I_n(m)$ denote the image of $X_m \to X_n$. Show that, for a fixed value of n, the set $I_n(m)$ is independent of m when m is large enough.
b) Let I_n be the common value of the $I_n(m)$ for m large. Show that, if $n \geqslant n'$, the image of the map $I_n \to X_n \to X_{n'}$ is $I_{n'}$.
c) Suppose that all the X_n are $\neq \varnothing$. Show that the same is true for the I_n. Conclude that $\varprojlim X_n = \varprojlim I_n \neq \varnothing$.
d) Give a topological proof of c) by viewing $\varprojlim X_n$ as the intersection of a decreasing family of nonempty closed subspaces of the compact space $\prod X_n$. [For a generalization, see Bourbaki [7], chap.I, §9.6.]
e) If, instead of being finite, the X_n are infinite, give an example where $\varprojlim X_n$ is empty.

14. With the notation of th.4.25, show that any two liftings $\rho_0 = (\rho_n)$ and $\rho_0' = (\rho_n')$ of ρ are conjugate.
[Hint: apply exerc.13 c) to $\varprojlim X_n$, where X_n is the set of elements $x \in \mathrm{GL}_N(\mathbf{Z}/p^n\mathbf{Z})$ such that $\mathrm{int}_x \circ \rho_n = \rho_n'$.]

15. (*Essential extensions.*) An extension $1 \to A \to E \to G \to 1$ is called *essential* if there is no proper subgroup of E which maps onto G. Suppose that E is essential and finite.
a) Let p be a prime number, and let A_p be a p-Sylow subgroup of A. Show that A_p is normal in E.
[Hint: use the Frattini argument.]
b) Show that A is nilpotent.
c) Show that $A_p = 1$ if p does not divide $|G|$.
[Hint: apply prop.4.22.]

Chapter 5

Hall subgroups

This chapter gives a generalization of Sylow's theorems for finite solvable groups: if G is such a group, and if a is a factor of $|G|$ which is prime to $|G|/a$, then there exists a subgroup A of G with $|A| = a$; moreover, just as in Sylow's theorem, the subgroup A is unique, up to G-conjugation.

5.1 π-subgroups

Let $\mathcal{P}$ be the set of all prime numbers. Let π be a subset of $\mathcal{P}$ and let $\pi' = \mathcal{P} - \pi$. An integer is called a π-integer if all its prime divisors belong to π. If n is an integer $\geqslant 1$, it can be written uniquely n as $n = n_\pi n_{\pi'}$, where n_π is a π-integer and $n_{\pi'}$ is a π'-integer.

A finite group is called a **π-group** if its order is a π-integer.

Definition 5.1. *Let G be a finite group and let π be a set of prime numbers. A subgroup H of G is called a **π-Sylow** subgroup (or a **Hall π-subgroup**) of G if $|H| = |G|_\pi$.*

In other words, a π-Sylow subgroup is a π-subgroup whose index is a π'-integer.

Example. If $\pi = \{p\}$, a π-Sylow subgroup of G is a p-Sylow subgroup of G.

Theorem 5.1 (P. Hall). *Let G be a finite solvable group and let π be a set of prime numbers. Then :*

(1) *G contains a π-Sylow subgroup.*

(2) *Let S be a π-Sylow subgroup of G, and let H be a π-subgroup of G. Then H is contained in a conjugate of S.*

The proof will be given in §5.4.

Corollary 5.2. *Two π-Sylow subgroups of a solvable group are conjugate.*

The next theorem shows that the solvability assumption of th.5.1 is essential :

Theorem 5.3. *If, for every set π of prime numbers, G contains a π-Sylow subgroup, then G is solvable.*

The proof will be given in §5.7. It relies on the following theorem, which will be proved in chap.8 (see th.8.21), using character theory:

Theorem 5.4 (Burnside). *Let p and q be two prime numbers. If G is a finite group of order $p^a q^b$ with $a, b \geqslant 0$, then G is solvable.*

5.2 Preliminaries: permutable subgroups

We first give a few lemmas on products of subgroups.

Recall that, if A and B be two subsets of a group G, we denote by AB the set of all products ab for $a \in A$ and $b \in B$.

Lemma 5.5. *If A and B are two subgroups of a group G, the following properties are equivalent :*

(1) $AB = BA$.

(2) *AB is a subgroup of G.*

Proof of (1) $\Longrightarrow$ (2). If $AB = BA$, we have $ABAB = AABB = AB$ and $(AB)^{-1} = BA = AB$; thus, AB is a subgroup of G.

Proof of (2) $\Longrightarrow$ (1). If AB is a subgroup of G, then $AB = (AB)^{-1} = BA$.

Two subgroups A and B are said to be **permutable** if $AB = BA$.

Examples.
1) If A normalizes B, or if B normalizes A, then A and B are permutable.
2) Let $G = \mathcal{S}_4$, let $A = \mathcal{S}_3$ and let B be a cyclic subgroup of order 4 of G. Then $AB = G$, which shows that A and B are permutable, even though neither of them normalizes the other one. For other such examples, see exerc.1.

Lemma 5.6. *Let $A_1, \ldots, A_n$ be subgroups of a group G that are pairwise permutable. Then $A_1 \cdots A_n$ is a subgroup of G.*

Proof. The proof is by induction on n. Lemma 5.5 gives the case $n = 2$. According to the induction hypothesis, $A_1 \cdots A_{n-1}$ is a subgroup. It is permutable with A_n since $A_1 \cdots A_{n-1}.A_n = A_1 \cdots A_n.A_{n-1} = \cdots$ (iterating $(n-1)$ times) $\cdots = A_n.A_1 \cdots A_{n-1}$. By lemma 5.5, $A_1 \cdots A_n$ is a subgroup of G.

Proposition 5.7. *Let A and B be two subgroups of a group G. The following properties are equivalent :*

(1) $AB = G$.
(1′) *A acts transitively on G/B.*
(2) $BA = G$.
(2′) *B acts transitively on G/A.*
(3) *The map $G \to G/A \times G/B$ is surjective.*
(3′) *G acts transitively on $G/A \times G/B$.*

Moreover, if $(G : A)$ and $(G : B)$ are finite, these properties are equivalent to each of the following :
(4) $(G : A \cap B) = (G : A)\,(G : B)$.
(4′) $(G : A \cap B) \geqslant (G : A)\,(G : B)$.

Proof. The equivalences (1) $\Longleftrightarrow$ (1′), (2) $\Longleftrightarrow$ (2′), and (3) $\Longleftrightarrow$ (3′) are clear.

(1) $\Longleftrightarrow$ (2). If $AB = G$, then AB is a subgroup of G; by lemma 5.5, we have $AB = BA$; thus, $BA = G$.

(1) $\Longrightarrow$ (3). We have to show that, given $g_1, g_2 \in G$, there exists $g \in G$ such that $g \in g_1A$ and $g \in g_2B$. By hypothesis, there exist $a \in A$ and $b \in B$ such that $g_1^{-1}g_2 = ab$, so we have $g_1a = g_2b^{-1}$; thus $g = g_1a = g_2b^{-1}$ is the desired element.

(3) $\Longrightarrow$ (1). If the group G acts transitively on $G/A \times G/B$, then, for every $g_1 \in G$, there exists $g \in G$ such that $g \in 1.A$ and $g \in g_1B$. This implies $g_1 \in AB$, i.e., $AB = G$.

Suppose now that G/A and G/B are finite. Let us show that (3) $\Longleftrightarrow$ (4). Let $\bar{1}$ be the image of the identity element of G in G/A (and G/B). The stabilizer of $(\bar{1}, \bar{1}) \in G/A \times G/B$ under the action of G is $A \cap B$. Let n be the number of elements in the orbit of $(\bar{1}, \bar{1})$; it is the index $(G : A \cap B)$ of $A \cap B$ in G. On the other hand,

$$\begin{aligned} G \text{ acts transitively on } G/A \times G/B &\Longleftrightarrow n = (G : A)(G : B) \\ &\Longleftrightarrow (G : A \cap B) = (G : A)(G : B), \end{aligned}$$

which shows that (3) and (4) are equivalent.

(4) $\Longleftrightarrow$ (4′). Since $(G : A \cap B)$ is the number of elements of the orbit of $(\bar{1}, \bar{1})$, it is bounded by $G/A \times G/B$, which is equal to $(G : A)(G : B)$.

Corollary 5.8. *If the indices of A and B in G are finite and relatively prime, then the properties* (1) *to* (4′) *of prop.5.7 hold.*

Proof. Indeed, $(G : A \cap B)$ is divisible by $(G : A)$ and $(G : B)$, and hence by their product; this shows that property (4′) holds.

5.3 Permutable families of Sylow subgroups

Let G be a finite group. For every prime p, let H_p be p-Sylow of G. The family $\{H_p\}$ is called **permutable** if the H_p are pairwise permutable in the sense defined in §5.2. In

that case, if π is a set of primes, lemma 5.6 shows that $H_\pi = \prod_{p \in \pi} H_p$ is a π-subgroup of G.

Theorem 5.9. *If G is solvable, G has a permutable family of Sylow subgroups.*

Proof. The proof is by induction on $|G|$. The case $G = 1$ is trivial. Assume $G \neq 1$. By cor.3.3, there exist a prime p_0 and a nontrivial normal p_0-subgroup A of G. By the induction hypothesis, the group G/A has a permutable family $\{H'_p\}$ of p-Sylow subgroups. Let $H' = \prod_{p \neq p_0} H'_p$; it is a subgroup of G/A of order $\prod_{p \neq p_0} |H'_p|$. Let G' be the inverse image of H' in G. We have an exact sequence :

$$1 \to A \to G' \to H' \to 1.$$

Since the orders of A and H' are relatively prime, there exists a subgroup H of G that lifts H', cf. th.4.6. For $p \neq p_0$, let H_p be the subgroup of H that lifts H'_p. The H_p are pairwise permutable p-Sylow subgroups of G. For $p = p_0$, define H_{p_0} to be the inverse image of H'_{p_0} in G. This is a p_0-Sylow subgroup of G. If $p \neq p_0$, the set $H_{p_0} H_p$ is the inverse image of $H'_{p_0} H'_p$, hence is a subgroup of G. This shows that H_{p_0} is permutable with the H_p for $p \neq p_0$. Then $\{H_p\}$ is the sought-after permutable family.

5.4 Proof of theorem 5.1

Assertion (1) (existence of π-Sylow subgroups) follows from th.5.9 and lemma 5.6.

We prove (2) by induction on $|G|$. Assume $G \neq 1$. Let S be a π-Sylow subgroup of G, and let H be a π-subgroup of G. We want to prove that H is contained in a conjugate of S. As in §5.3, choose a prime p_0 and a nontrivial normal p_0-subgroup A of G. Let H' and S' be the images of H and S in $G' = G/A$. By the induction hypothesis, H' is contained in a conjugate of S'. After replacing H' by one of its conjugates, we may thus assume that $H' \subset S'$. There are two cases:

1) $p_0 \in \pi$. Then $A \subset S$; indeed, S contains a p_0-Sylow subgroup S_0 of G and A is normal, hence $A \subset S_0$ (cf. th.2.6). The inclusion $H' \subset S'$ therefore gives $H \subset S$.

2) $p_0 \notin \pi$. Then the orders of A and S are relatively prime, hence $A \cap H = 1$ and $A \cap S = 1$. The projections $H \to H'$ and $S \to S'$ are isomorphisms. Let $\widetilde{H}$ be the subgroup of S that projects onto H'. Then the groups H and $\widetilde{H}$ are two liftings of H' in AH. Hence they are conjugate by part (2) of th.4.20.

5.5 Sylow-like properties of the π-subgroups

Propositions 2.10 and 2.11 also apply to π-subgroups, provided G is solvable :

Proposition 5.10. *Let G be a finite solvable group. Let H be a subgroup of G and let P be a π-Sylow subgroup of H. There exists a π-Sylow subgroup S of G such that $P = S \cap H$.*

Proof. This follows from part (2) of th.5.1 applied to P.

Proposition 5.11. *Let G be a finite solvable group. Let H be a normal subgroup of G and let S be a π-Sylow subgroup of G. Then :*
(1) $S \cap H$ is a π-Sylow subgroup of H.
(2) The image S' of S in G/H is a π-Sylow subgroup of G/H.
(3) Every π-Sylow subgroup of G/H is the image of a π-Sylow subgroup of G.
(4) If Q is a π-Sylow subgroup of H, then $HN_G(Q) = G$.

Proof.

(1) By prop.5.10 there exists a p-Sylow S' of G such that $S' \cap H$ is a π-Sylow subgroup of H. Since S and S' are conjugate, and H is normal, $S' \cap H$ and $S \cap H$ are G-conjugate, hence have the same order. This implies that $S \cap H$ is a π-Sylow subgroup of H.

(2) The index of S in G is a π'-integer; hence the same is true of the index of S' in G/H. Since S' is a π-group, this shows that S' is a π-Sylow subgroup of G/H.

(3) This follows from (2) since the π-Sylow subgroups of G/H are conjugate.

(4) Let $g \in G$. We have $gQg^{-1} \subset gHg^{-1} = H$. Since gQg^{-1} has the same order as Q, it is a π-Sylow subgroup of H; by cor.5.2, there exists $h \in H$ such that $gQg^{-1} = hQh^{-1}$. Hence, $h^{-1}g \in N_G(Q)$ and $g \in HN_G(Q)$. This shows that $HN_G(Q) = G$.

5.6 A solvability criterion

Theorem 5.12 (Wielandt). *Let G be a finite group. Let H_1, H_2, H_3 be subgroups of G. If the H_i are solvable, and if their indices in G are pairwise prime, then G is solvable.*

Proof. Use induction on $|G|$.

First, since the indices $(G : H_1)$ and $(G : H_2)$ are relatively prime, by cor.5.8, we have $G = H_1H_2$.

We may assume $H_1 \neq 1$. By cor.3.3, there exist a nontrivial normal p-subgroup A of H_1 for some prime number p. The prime p divides at most one of the indices of H_2 and H_3. After possibly renumbering H_2 and H_3, we may assume that p does not divide $(G : H_2)$. Then H_2 contains a Sylow p-subgroup of G; hence, it contains a conjugate of A. Since $G = H_1H_2$, and A is normal in H_1, every conjugate of A is of the form $h^{-1}Ah$ with $h \in H_2$. Moreover, since a conjugate of A is contained in H_2, all the conjugates of A are contained in H_2. Let $\widetilde{A}$ be the subgroup of G generated by the conjugates of A. Then $\widetilde{A}$ is normal in G and is contained in H_2, hence is solvable. Let H_i' be the images of H_i in $G' = G/\widetilde{A}$. The indices $(G' : H_i')$ are pairwise prime (since $(G' : H_i')$ divides $(G : H_i)$) and the H_i' are solvable. The induction hypothesis shows that G' is solvable; since G is an extension of two solvable groups, it is solvable.

5.7 Proof of theorem 5.3

Let p be a prime number and let G be a finite group. A subgroup of G is called a **p-complement** if it is a p'-Sylow subgroup, where $p' = \mathcal{P} - \{p\}$. (Recall that $\mathcal{P}$ denotes the set of all prime numbers.)

We prove a stronger version of theorem 5.3 :

Theorem 5.13. *If G has a p-complement for every prime p, then G is solvable.*

Proof.
Use induction on $|G|$. By Burnside's theorem (th.5.4), we may assume that $|G|$ has at least three distinct prime factors, p_1, p_2, p_3. For $i = 1, 2, 3$, let H_i be a p_i-complement of G. Then the indices $(G : H_i)$ for $i = 1, 2, 3$ are pairwise relatively prime. Moreover, H_i has a p-complement for every prime p. Indeed, if $p = p_i$, then H_i is its own p_i-complement. If $p \neq p_i$, let H_p be a p-complement for G; since $(G : H_i)$ and $(G : H_p)$ are relatively prime, lemma 5.8 shows that

$$(G : H_i \cap H_p) = (G : H_i)(G : H_p),$$

hence $(H_i : H_i \cap H_p)$ is the highest power of p dividing $|H_i|$. Since $H_i \cap H_p$ is a p'-group, $H_i \cap H_p$ is a p-complement of H_i. By the induction hypothesis, H_i is solvable. We have shown that G satisfies the hypotheses of th.5.12; hence G is solvable.

5.8 Exercises

1. (*Examples of subgroups A, B of G such that $G = AB$ without either A or B being normal in G.*)
   a) Let $H = CD$, where C is not normal in H, e.g. $H = \mathcal{S}_3$, C of order 2 and D of order 3. Let $G = H \times H, A = C \times D$ and $B = D \times C$. Show that $G = AB$ and that neither A nor B is normal in G.
   b) Let p be a prime number. Let $G = \mathrm{PGL}_2(\mathbf{F}_p)$, let A be the upper triangular subgroup of G of order $p(p-1)$ and let B be a cyclic subgroup of G of order $p+1$. Show that $G = AB$. Show that neither A nor B is normal in G when $p \neq 2$.

2. (*Bicyclic groups.*) Let $G = AB$ be a group which is the product of two cyclic subgroups A and B.
   a) Suppose that $G \neq 1$. Show that G has a nontrivial normal subgroup which is cyclic. [Hint: this is clear if $A \cap B \neq 1$. We may assume that $A \cap B = 1$, and also that $|A| \geqslant |B|$. Let b be a generator of B. For every $a \in A$, choose $\beta(a) \in B - \{1\}$ such that $ab \in \beta(a)A$. The map $\beta : A \to B - \{1\}$ is not injective. Choose two distinct elements a_1, a_2 such that $\beta(a_1) = \beta(a_2)$. Put $a = a_2^{-1}a_1$. Show that $b^{-1}ab \in A$; the subgroup of A generated by a is a nontrivial normal cyclic subgroup of G.]
   b) Show that G is supersolvable (cf. chap.3, exerc.13).
   [Hint: use a) together with induction on the order of G.]

3. Let G be a supersolvable finite group.
   a) Let $\mathcal{P}_G$ denotes the set of all prime divisors of $|G|$. Let π be a subset of $\mathcal{P}_G$ such that $p \in \pi$ and $q \in \mathcal{P}_G - \pi$ implies $q \not\equiv 1 \pmod{p}$. Show that G has a unique π-Sylow subgroup.
   [Hint: use part e) of chap.3, exerc.13.]
   b) Show that, if d is a divisor of $|G|$, there exists a subgroup of G of order d.
   [Hint: use induction on $|G|$ and assume $|G| > 1$. Choose a normal subgroup N of G of prime order; let p be its order. If p divides d, apply the induction hypothesis to G/N. If p does not divide d, apply the induction hypothesis to a p'-Sylow subgroup of G.]

Chapter 6

Frobenius groups

6.1 Union of conjugates of a subgroup

Lemma 6.1. *Let H be a subgroup of a finite group G. Let H^{cl} be the union of the conjugates of H. Then :*

a) $|G| - |H^{\mathrm{cl}}| \geqslant n - 1$, *where* $n = (G : H)$.

b) There is equality in a) if and only if $H \cap gHg^{-1} = 1$ *for every* $g \in G - H$.

Proof. Let $X = G/H$; we have $|X| = n$; if $x \in X$, denote by G_x the stabilizer of x. We have

$$H^{\mathrm{cl}} = \{1\} \cup \bigcup_{x \in X} (G_x - \{1\}).$$

Since G_x is a conjugate of H, this gives $|H^{\mathrm{cl}}| \leqslant 1 + n(|H| - 1) = 1 + |G| - n$. There is equality if and only if the sets $G_x - \{1\}$ are disjoint; this is equivalent to $H \cap gHg^{-1} = 1$ for every $g \in G - H$.

Remark. The bound for $|H^{\mathrm{cl}}|$ given in a) can be improved to the following one (due to P.J. Cameron and A.M. Cohen, [47]):

$$\frac{|H^{\mathrm{cl}}|}{|G|} \leqslant 1 - \frac{1}{n}.$$

For the proof, and further information and examples, see [47], [72], and exerc.1.

Theorem 6.2 (Jordan [61]). *Let X be a finite set on which a group G acts transitively. Assume $|X| \geqslant 2$. Then there exists an element of G which fixes no element of X.*

Proof. By replacing G by its image in $\mathcal{S}_X$ we may assume that G is finite. Let H be the stabilizer of a point of X. Part a) of lemma 6.1 shows that $|G| - |H^{\mathrm{cl}}| > 0$, hence that there exists an element of G which is not conjugate to any element of H, i.e., which has no fixed point.

Equivalent formulation:

Theorem 6.3. *Let H be a subgroup of finite index of a group G. If H intersects every conjugacy class of G, then $H = G$.*

Remark. The assumption that $(G : H) < \infty$ cannot be dropped. Consider, for example, $G = \mathbf{SO}_3(\mathbf{R})$ and $H = \mathbf{U}(1)$ = group of rotations with a given axis: every element of G is a rotation, hence is conjugate to an element of H. [Generalization: G = compact connected Lie group and H = maximal torus of G.]

Here are two applications of th.6.3:

1) *Every finite division ring is commutative (Wedderburn theorem).*

   Let D be a finite division ring and let F be its center. It is known[1] that $[D : F]$ is a square and that every $x \in D$ is contained in a subfield L of D containing F such that $[L : F]^2 = [D : F]$; two such fields are isomorphic, since they have the same number of elements, hence they are conjugate by an inner automorphism of D (Skolem-Noether theorem). Fix such an L. Let $G = D^\times$ and $H = L^\times$. We have $G = \bigcup_{g \in G} gHg^{-1}$. Theorem 6.3 implies that $G = H$, i.e., $D = L$, hence D is commutative.

2) *Roots of a polynomial after reduction modulo p.*

   Let $f = x^n + a_1 x^{n-1} + \cdots + a_n \in \mathbf{Z}[x]$ be a monic polynomial of degree $n > 1$, which is irreducible over $\mathbf{Q}$. If p is a prime number, let $f_p \in \mathbf{F}_p[x]$ be the image of f by reduction modulo p. Let $\mathcal{P}_f$ be the set of p such that f_p has at least one root in $\mathbf{F}_p$. Let $X = \{x_1, \ldots, x_n\}$ be the set of roots of f in an extension of $\mathbf{Q}$ and let G be the Galois group of f, i.e., the group of automorphisms of the extension $\mathbf{Q}(x_1, \ldots, x_n)/\mathbf{Q}$. The group G acts transitively on X; thus, $X \simeq G/H$, where H is the stabilizer of x_1. The Chebotarev-Frobenius theorem (see e.g. [72] and the references given there) implies that the density[2] of $\mathcal{P}_f$ exists and is equal to $|H^{\mathrm{cl}}|/|G|$. Since $H \neq G$ (because $n > 1$), th.6.3 shows that this density is < 1. Hence *there exist infinitely many primes p such that f_p has no root in $\mathbf{F}_p$*; more precisely, the set of such primes has a density which is $\geqslant 1/n$, cf. exerc.1.

6.2 An improvement of Jordan's theorem

Let (G, H) be a pair as in the preceding section, i.e., G finite, $H \subset G$ and $(G : H) > 1$. By Jordan's theorem, there exists $g \in G$ which is not conjugate to any element of H. There are questions (see below) where a further property of g is needed, namely that *its order is a power of a prime number.* This innocuous-looking condition is much more difficult to meet than one would think. But it can be met, according to [52]. Indeed, that paper contains the following statement:

[1] For the proofs of the results used below, see e.g. Bourbaki [5], §14.

[2] If P is a set of prime numbers, and if d is a positive real number, one says that P has density d if $|\{p \leqslant x,\ p \in P\}|/|\{p \leqslant x\}| \to d$ as $x \to +\infty$.

Theorem 6.4. *If H is a proper subgroup of a finite group G, there exists an element of G, of prime power order, which does not belong to any conjugate of H.*

The reader should be warned that the proof given in [52] is not complete: it is by reduction to the case where G is simple, which is handled by appealing not only to CFSG but also to " published and unpublished " properties of the sporadic groups.

Application to finite extensions of number fields

Let K/k be a finite extension of algebraic number fields of degree > 1, and let L/k be a finite Galois extension of k containing K. Put $G = \mathrm{Gal}(L/k)$ and $H = \mathrm{Gal}(L/K)$. Then:

Theorem 6.5 ([52], [75]). *The following properties are equivalent :*
(1) *Theorem* 6.4. *is true for* (G, H).
(2) *The kernel of the map* $\mathrm{Br}(k) \to \mathrm{Br}(K)$ *is infinite.*
(3) *The group* $k^\times/N_{K/k}K^\times$ *is infinite.*
[Here $\mathrm{Br}(k)$ and $\mathrm{Br}(K)$ denote the Brauer groups of k and of K, cf. Bourbaki [5], §15 and §16, and $N_{K/k} : K^\times \to k^\times$ is the norm map.]

The proof gives the following more precise result :

Theorem 6.6. *Let p be a prime number. The following properties are equivalent :*
(1) *There exists an element of G, of order a power of p, which is not conjugate to any element of H.*
(1′) *There exists a cyclic subgroup C of G such that the order of every orbit of C in G/H is divisible by p.*
(1″) *Let O_k (resp. O_K) be the ring of integers of k (resp. of K); there exists infinitely many prime ideals $\mathfrak{q}$ of O_k such that $\mathfrak{q}O_K$ is the p-th power of an ideal of O_K.*
(2) *The p-component of* $\mathrm{Ker}(\mathrm{Br}(k) \to \mathrm{Br}(K))$ *is infinite.*
(3) *The p-component of* $k^\times/N_{K/k}K^\times$ *is infinite.*

Note. The equivalence of (1) and (1′) is easy. That of (1′) and (1″) is a consequence of Chebotarev's density theorem, cf. [65]. That of (1″), (2) and (3) uses standard properties of number fields and Brauer groups.

6.3 Frobenius groups: definition

We now look at the pairs (G, H) for which the inequality a) of 6.1 is an equality, i.e.,

$$|H^{\mathrm{cl}}| = |G| - (G : H) + 1, \tag{6.1}$$

or equivalently :

$$H \cap gHg^{-1} = 1 \text{ for every } g \in G - H. \tag{6.2}$$

Let $X = G/H$. Property 6.2 can be restated as saying that *every element of G different from the identity fixes at most one point of X*; in other words, the only element of G that fixes two points is the identity.

[Property 6.2 is sometimes expressed by saying that H is *malnormal*, i.e., very far from normal; note that this makes sense without any finiteness assumption on G, H, or X; see de la Harpe - Weber [58] for interesting examples involving infinite groups.]

Definition 6.1. *A pair (G, H) is called a* ***Frobenius pair*** *if it has properties 6.1 and 6.2 above; it is called* ***nontrivial*** *if H is different from 1 and from G.*
A finite group G is called a ***Frobenius group*** *if it contains a subgroup H such that (G, H) is a nontrivial Frobenius pair.*

Examples.

1. Let n be an odd integer $\geqslant 3$. The dihedral group $\mathcal{D}_n$ of order $2n$ is a Frobenius group, as one sees by taking H of order 2.

2. Let F be a finite field, and let G be the group of affine linear maps $g_{a,b} : x \mapsto ax+b$, with $a \in F^\times$ and $b \in F$. Let H be the stabilizer of 0, i.e., the group of homotheties $g_{a,0} : \{x \mapsto ax\}$. The pair (G, H) is a Frobenius pair; indeed, a nontrivial element $g_{a,b}$ of G has, either no fixed point if $a = 1$, or one fixed point if $a \neq 1$.

3. Let N and H be two finite groups, and let $h \mapsto \sigma_h$ be a homomorphism of H into $\mathrm{Aut}(N)$. Let G be the corresponding semidirect product $N \rtimes H$. We have $\sigma_h(x) = hxh^{-1}$ if $h \in H$ and $x \in N$. The pair (G, H) is a Frobenius pair if and only if $H \cap xHx^{-1} = 1$ for all $x \in N - \{1\}$. A simple computation shows that this means that $\sigma_h(x) = x$ only when $h = 1$ or $x = 1$; equivalently: *H acts freely on $N - \{1\}$.*

   Note that, in such a case, we have:

$$N = \{1\} \cup (G - H^{\text{cl}}), \quad \text{i.e.,} \quad H^{\text{cl}} = \{1\} \cup (G - N). \tag{6.3}$$

It is a remarkable fact that Example 3 above gives *all* the Frobenius pairs:

Theorem 6.7 (Frobenius [19], p.199). *Let (G, H) be a Frobenius pair. Then the identity, together with the elements of G which do not belong to any conjugate of H, make up a normal subgroup N of G such that $N \cap H = 1$ and $G = NH$.*

[Hence G is the semidirect product of H and N.]

Proof. The main point is to show that the set $N = \{1\} \cup (G - H^{\mathrm{cl}})$ is a subgroup of G; the proof, which uses character theory, will be given in chap.8 (th.8.54). The other statements are easy:

The group N is obviously invariant under conjugation; it is also clear that $N \cap H = 1$. By 6.1, we have $|G - H^{\mathrm{cl}}| = (G : H) - 1$, hence $|N| = (G : H)$. Finally, from $N \cap H = 1$, we obtain $G = NH$.

Remark. A group G can be a Frobenius group in "only one way": if (G, H_1) and (G, H_2) are nontrivial Frobenius pairs, then H_1 and H_2 are conjugate, cf. exerc.6. In particular, the normal subgroup N is unique; it is called the **Frobenius kernel** of G, while H, which is unique up to conjugation, is called the **Frobenius complement**.

We shall now look at the structures of N and H.

6.4 Frobenius kernels

Let (G, H) be a nontrivial Frobenius pair and let N be the corresponding Frobenius kernel. Choose $x \in H$ of prime order p. The element x defines an automorphism σ of N of order p without fixed point other than 1. Conversely, if N has such an automorphism, the semidirect product of $\mathbf{Z}/p\mathbf{Z}$ and N is a Frobenius group with kernel N. Hence:

Proposition 6.8. *A nontrivial finite group N is a Frobenius kernel if and only if there exists an automorphism of N, of prime order, which has no fixed point $\neq 1$.*

Such a group has the following properties:

Proposition 6.9. *Let σ be an automorphism of order p (not necessarily prime) of a finite group N. Suppose that 1 is the only fixed point of σ. Then :*

(1) *The map $x \mapsto x^{-1}\sigma(x)$ of N into N is bijective.*

(2) *If x and $\sigma(x)$ are conjugate in N, then $x = 1$.*

(3) *For every $x \in N$, we have $x\sigma(x)\sigma^2(x)\cdots\sigma^{p-1}(x) = 1$.*

Proof.

(1) Since N is finite, it is enough to show that the map $x \mapsto x^{-1}\sigma(x)$ is injective. Suppose that $x^{-1}\sigma(x) = y^{-1}\sigma(y)$ with $x, y \in N$. Thus, $yx^{-1} = \sigma(yx^{-1})$. Therefore, the element yx^{-1} is fixed by σ. By assumption, we have $yx^{-1} = 1$, i.e., $x = y$.

(2) Let $x \in N$. Suppose that there exists $a \in N$ such that $\sigma(x) = axa^{-1}$. By (1), there exists $b \in N$ such that $a^{-1} = b^{-1}\sigma(b)$. Then $\sigma(x) = \sigma(b)^{-1}bxb^{-1}\sigma(b)$, and hence $\sigma(bxb^{-1}) = bxb^{-1}$, which implies $bxb^{-1} = 1$ and $x = 1$.

(3) Let $a = x\sigma(x)\sigma^2(x)\cdots\sigma^{p-1}(x)$. We have $\sigma(a) = \sigma(x)\sigma^2(x)\cdots\sigma^{p-1}(x)x = x^{-1}ax$, hence $a = 1$, thanks to (2).

Corollary 6.10. *If ℓ is a prime number, there exists an ℓ-Sylow subgroup of N which is stable under the action of σ.*

Proof. Let S be an ℓ-Sylow subgroup of N. The group $\sigma(S)$ is also an ℓ-Sylow subgroup of N, hence there exists $a \in N$ such that $aSa^{-1} = \sigma(S)$. According to prop.6.9 (1), we can write a^{-1} in the form $a^{-1} = b^{-1}\sigma(b)$, hence $\sigma(b^{-1})bSb^{-1}\sigma(b) = \sigma(S)$, which implies $bSb^{-1} = \sigma(b)\sigma(S)\sigma(b^{-1}) = \sigma(bSb^{-1})$. Therefore, bSb^{-1} is a σ-stable ℓ-Sylow subgroup of N.

Corollary 6.11. *If $a \in N$, the automorphism $\sigma_a = \mathrm{int}_a \circ \sigma : x \mapsto a\sigma(x)a^{-1}$ is conjugate to σ in* $\mathrm{Aut}(G)$; *in particular, it is of order p and it has no fixed point $\neq 1$.*

Proof. According to prop.6.9 (1), there exists $b \in G$ such that $a = b^{-1}\sigma(b)$; then $\sigma_a(x) = b^{-1}\sigma(bxb^{-1})b$, hence $b\sigma_a(x)b^{-1} = \sigma(bxb^{-1})$, i.e., $\mathrm{int}_b \circ \sigma_a = \sigma \circ \mathrm{int}_b$. This shows that σ and σ_a are conjugate.

Examples.

1. If $p = 2$, we have $x\sigma(x) = 1$ for all $x \in N$, hence $\sigma(x) = x^{-1}$. Since σ is an automorphism, N is abelian.

2. In the case $p = 3$, let $\sigma(x) = x'$ and $\sigma^2(x) = x''$. Proposition 6.9 (3) applied to σ and σ^2 gives $xx'x'' = 1$ and $xx''x' = 1$, hence x' commutes with x''; by similar reasoning, we see that x, x' and x'' commute. Similarly, for all a, x commutes with $ax'a^{-1}$, and x commutes with $ax''a^{-1}$. Therefore, x' and x'' commute with all conjugates of x; since $x = (x'x'')^{-1}$ the same is true for x. Hence N has the following property: any two conjugate elements commute; equivalently x commutes with the commutator (x, y) for every y, i.e., $\big(x, (x, y)\big) = 1$ for all $x, y \in N$. Using this information, Burnside has shown (cf. [46]) that N is nilpotent of nilpotency class $\leqslant 2$.

3. The case $p = 5$ has been treated by G. Higman [60]: the group N is nilpotent of nilpotency class $\leqslant 6$ (the bound is best possible).

4. For an arbitrary prime p, Higman proved that, if N is solvable, then it is nilpotent. He also conjectured that the nilpotency class of N is $\leqslant \frac{p^2-1}{4}$, which would be best possible; see also L. Wilson's report [80].

These results led to the conjecture that every Frobenius kernel is a nilpotent group. This was settled in 1960 by J.G. Thompson in his thesis [78]:

Theorem 6.12. *Every Frobenius kernel is nilpotent.*

For a proof, see [78] and Huppert [25], Kap.V, Haupsatz 8.14.

Remark. There is an analogous (but easier) result for Lie algebras, due to N. Jacobson: a finite dimensional Lie algebra over a field, which has an automorphism of prime order with no fixed point $\neq 0$, is nilpotent (cf. Bourbaki [8], chap.I, §4, exerc.21).

6.5 Frobenius complements

Let us say that a group H has property $\mathcal{F}$ *if there exists a group G strictly containing H such that (G, H) is a Frobenius pair.*

According to th.6.7 and th.6.12, this means that there exists a nilpotent group $N \neq 1$ on which H acts **almost freely** [3], i.e., freely on $N - \{1\}$.

Example. Let K be a finite field of characteristic p and let H be a subgroup of $\mathbf{SL}_2(K)$ whose order is relatively prime to p. Let N be the vector space K^2 over K. The group H acts almost freely on N; indeed, if a nontrivial element $h \in H$ has 1 as eigenvalue, its other eigenvalue is also 1, hence h is conjugate to $\left(\begin{smallmatrix}1 & \lambda \\ 0 & 1\end{smallmatrix}\right)$ for some $\lambda \in K$, hence has order p; this contradicts our assumption on $|H|$. Therefore, H has property $\mathcal{F}$.

Theorem 6.13. *Let H be a finite group. The following properties are equivalent :*

(1) *H has property $\mathcal{F}$.*

(2) *There exist a field K and a linear representation*[4] *$\rho : H \to \mathbf{GL}_n(K)$, with $n \geqslant 1$, which is almost free , i.e., such that H acts freely on $K^n - \{0\}$.*

(3) *For every field K whose characteristic does not divide $|H|$, there exists a linear representation $\rho : H \to \mathrm{GL}_n(K)$, with $n \geqslant 1$, which is almost free.*

(4) *There exists a linear irreducible representation $\rho : H \to \mathrm{GL}_n(\mathbf{C})$ which is almost free.*

(5) *It is possible to make H act freely, by orthogonal transformations, on the unit sphere $\mathbf{S}_{n-1}$ of the Euclidean space $\mathbf{R}^n$, for some $n \geqslant 1$.*

(Note that (2) and (3) imply that ρ is faithful.)

Proof of theorem 6.13. First part.

If K is a field, we shall say that it has "property (2_K)" (relative to H) if:

(2_K) *There exists an integer $n > 0$ and an almost free representation $H \to \mathrm{GL}_n(K)$.*

We shall need several results on (2_K) :

(a) *Property (2_K) depends only on the characteristic of K.*

Let K be a field having property (2_K), and let x be a nonzero element of K^n. The H-orbit of x generates a finite dimensional vector space over the prime field K_0 (i.e., $\mathbf{F}_p$ or $\mathbf{Q}$); let n be its dimension; we thus obtain a representation $H \to \mathrm{GL}_n(K_0)$ which is almost free. If K_1 is an extension of K_0, the representation $H \to \mathrm{GL}_n(K_0) \to \mathrm{GL}_n(K_1)$ is almost free (e.g. because no element of $G - \{1\}$ has an eigenvalue equal to 1). This shows that (2_K) holds for every field of the same characteristic as K.

[3]Many authors speak of a "fixed point free" action, which can be confusing.

[4]In this section, and in the related exercises, we use the elementary properties of the linear representations which will be given in chap.8.

(*b*) *If* (2_K) *is true, the characteristic of* K *cannot be a prime number dividing* $|H|$.
Indeed, if H acts freely on $\mathbf{F}_p^n - \{0\}$, the order of H divides $p^n - 1$ and is therefore not divisible by p.

(*c*) *If property* (2_K) *holds in characteristic* 0*, it holds in every characteristic* p *not dividing* $|H|$.
According to (*a*), there exists a finite dimensional vector space V over $\mathbf{Q}$ with $\dim V \geqslant 1$ on which H acts almost freely. Let $x \in V$ be a nonzero vector and let L be the subgroup of V generated by the H-orbit of x. The group H acts on L, hence also on the $\mathbf{F}_p$-vector space $V_p = L/pL$. Let us show that this action is almost free, provided that p does not divide $|H|$. If $s \in H$ has order $m > 1$, the automorphism s_V of V defined by s is such that $s_V^m = 1$, and it does not has 1 as an eigenvalue. Therefore, we have

$$1 + s_V + s_V^2 + \cdots + s_V^{m-1} = 0.$$

A fortiori, the same equation holds in V_p and it implies $s_{V_p}x \neq x$ for all nonzero $x \in V_p$ (since m is prime to p). Hence, property (2_K) holds for $\mathbf{F}_p$.

(*d*) *If property* (2_K) *holds in characteristic* $p \neq 0$*, it holds in characteristic* 0.
Let $\rho : H \to \mathbf{GL}_n(\mathbf{Z}/p\mathbf{Z})$ be an almost free linear representation of H over $\mathbf{F}_p$. By (*b*), p does not divide $|H|$. Theorem 4.25 shows that we can lift ρ to a homomorphism $H \to \mathbf{GL}_n(\mathbf{Z}_p)$, where $\mathbf{Z}_p$ is the ring of p-adic integers. Since $\mathbf{Z}_p \subset \mathbf{Q}_p$, we obtain a linear representation $H \to \mathbf{GL}_n(\mathbf{Q}_p)$ in characteristic zero. This representation is almost free. Indeed, if $x = (x_1, \ldots, x_n)$ is a nonzero vector fixed by $h \in H$, with $h \neq 1$, we may suppose (after multiplying x by a scalar) that the x_i belong to $\mathbf{Z}_p$ and that one of them is not divisible by p. The reduction of x modulo p therefore yields a nonzero vector of $\mathbf{F}_p^n$ fixed by h, contradicting the hypothesis.

Proof of theorem 6.13. Second part.

It follows from (*a*), (*b*), (*c*) and (*d*) that (2_K) is independent of K, provided the characteristic of K is not a prime factor of $|H|$. Hence $(2) \Longleftrightarrow (3)$.

We now prove the other equivalences:

$(3) \Longleftrightarrow (4)$ By (3), applied to $\mathbf{C}$, there exists a nonzero complex representation of H which is almost free; by taking an irreducible subrepresentation, we obtain (4). Conversely, it is clear that $(4) \Longrightarrow (2)$, hence $(4) \Longrightarrow (3)$.

$(1) \Longrightarrow (2)$ Suppose that H acts almost freely on a finite group $N \neq 1$. Since N is nilpotent (th.6.12), its center $Z(N)$ is nontrivial (cor.3.10). If p a prime factor of $|Z(N)|$, the group of elements $x \in Z(N)$ such that $x^p = 1$ is a nonzero vector space over $\mathbf{F}_p$ on which H acts almost freely.

$(3) \Longrightarrow (1)$ Choose such a finite field K. We obtain an almost free action of H on an elementary abelian group.

$(5) \Longrightarrow (2)$ Choose $K = \mathbf{R}$.

$(3) \Longrightarrow (5)$ Choose $K = \mathbf{R}$ and let $\rho : H \to \mathbf{GL}_n(\mathbf{R})$ be an almost free linear representation. Since H is finite, there exists a positive definite quadratic form on $\mathbf{R}^n$ invariant

under H (take for instance the sum of the H-transforms of $\sum x_i^2$). After conjugation, we may thus assume that $\rho(H)$ is contained in the orthogonal group $\mathbf{O}_n(\mathbf{R})$; hence it stabilizes the sphere $\mathbf{S}_{n-1}$ defined by the equation $\sum_{i=1}^{n} x_i^2 = 1$, and it acts freely on it. This completes the proof of the theorem.

Corollary 6.14. *If H has property $\mathcal{F}$, its abelian subgroups are cyclic.*

Proof. This means that an abelian group having property $\mathcal{F}$ is cyclic, which is clear from (4), since an irreducible representation of an abelian group is one-dimensional, cf. chap.8, cor.8.14.

It can be shown (Wolf [40], th.5.3.2) that property 6.14 implies that the p-Sylow subgroups of H are either cyclic groups or generalized quaternion groups (for the case $p \neq 2$, see exerc.6 of chap.4).

Remarks.

1. Property (5) can be restated in the language of Riemannian geometry as:

(5′) *H is the fundamental group of a compact connected Riemannian manifold of constant > 0 curvature.*

Indeed, such Riemannian manifolds are known to be the quotients S/H, where S is a sphere with its standard Riemannian structure, and H is a finite group acting freely on S by orthogonal transformations, cf. Wolf [40], cor.2.4.10. A classification of the possible groups H is given in chap.6 of [40]. In particular, these groups are either solvable, or contain a subgroup of index $\leqslant 2$ which is the direct product of $\mathrm{SL}_2(\mathbf{F}_5)$ by a solvable group ([40], th.6.3.1).

2. In part (5) of th.6.13, if we replace "orthogonal transformations" by "homeomorphisms", we get a larger family of finite groups: those which can act freely and topologically on a sphere. It is a theorem of I. Madsen, C.B. Thomas and C.T.C. Wall (see [66]) that a finite group H belongs to that enlarged family if and only if :

($\mathcal{F}_{\text{top}}$) *Every subgroup of H of order either $2p$ or p^2, with p prime, is cyclic.*

Note for instance that a nonabelian group of order pq, where p and q are odd primes, has this property; but it does not have property ($\mathcal{F}$), cf. exerc.9.

6.6 Exercises

1. (*Cameron-Cohen bound*, [47].) Let X be a finite set on which a finite group G acts transitively. Let $n = |X|$; assume $n \geqslant 2$. If $g \in G$, let $\chi(g) = |X^g|$ be the number of fixed points of g. Let G_0 be the set of all $g \in G$ such that $\chi(g) = 0$.
   a) Let
   $$S = \sum_{g \in G} (\chi(g) - 1)(\chi(g) - n).$$
   Show that $S \leqslant n|G_0|$.
   [Hint : split the sum into its G_0-part and its $(G - G_0)$-part.]

b) Show that $S \geqslant |G|$.
[Hint: use that $\sum_{g\in G} \chi(g) = |G|$ and $\sum_{g\in G} \chi(g)^2 \geqslant 2|G|$, by Burnside's lemma and chap.1, exerc.6.]
c) Deduce that $|G_0| \geqslant |G|/n$.
d) Show that, if there is equality in c), then G is a Frobenius group, for which the Frobenius complement H acts transitively and freely on $N - \{1\}$, where N is the Frobenius kernel. This implies that N is elementary abelian, hence that n is a power of a prime.

2. Let g be an element of a finite group G. Suppose that every conjugacy class of G contains an element which commutes with g. Show that g belongs to $Z(G)$.
[Hint: apply th.6.3 to a well-chosen subgroup of G.]

3. (*Small Frobenius groups.*) Show that a Frobenius group of order $\leqslant 30$ has order 6, 10, 12, 14, 18, 20, 21, 22, 26 or 30. [Use the fact that the order of a Frobenius group is of the form $n(1+an)$, with $n \geqslant 2$ and $a \geqslant 1$.] Show that, for every integer in this list, except 18, there exists a unique Frobenius group of that order, up to isomorphism. Show that there are two nonisomorphic Frobenius groups of order 18.
Show that a Frobenius group of odd order $\leqslant 100$ has order 21, 39, 55, 57, 75 or 93.

4. Show that the smallest nonsolvable Frobenius group as order 120×121, with Frobenius complement isomorphic to $\mathrm{SL}_2(\mathbf{F}_5)$.
[Hint : use the inclusion $\mathcal{A}_5 \subset \mathrm{PSL}_2(\mathbf{F}_{11})$, cf. chap.10, §2, to construct an embedding of $\mathrm{SL}_2(\mathbf{F}_5)$ into $\mathrm{SL}_2(\mathbf{F}_{11})$.]

5. Let (G, H) be a Frobenius pair, and let N be the corresponding Frobenius kernel. Let M be a normal subgroup of G. Show that either $M \supset N$ or $M \subset N$.
[Hint: suppose that M is not contained in N and choose $m \in M - N$. Since $m \notin N$, m is conjugate to an element of H, and the automorphism σ of N given by $z \mapsto mzm^{-1}$ has no fixed point $\neq 1$. By prop.6.9, every element x of N can be written as $x = z^{-1}\sigma(z)$ for some $z \in N$. Hence $x = z^{-1}mz.m^{-1}$. Since M is normal, we have $z^{-1}mz \in M$, hence $x \in M$; this shows that $N \subset M$.]

6. (*Uniqueness of the Frobenius structure.*) Let (G, H) and (G, H') be two nontrivial Frobenius pairs relative to the same group G, and let N, N' be the corresponding Frobenius kernels. Show that $N' = N$ and that H' is conjugate to H.
[Hint: By exerc.5, we may assume that $N \subset N'$. If $N' \neq N$, let x be an element of $N' - N$. Since x is conjugate to an element of H, its order divides $|N| - 1$, hence is prime to $|N|$. Since N' is nilpotent (th.6.12), this implies that x commutes with the elements of N; this contradicts the fact that int_x acts freely on $N - \{1\}$. Hence $N' = N$. Theorem 4.20 shows that H and H' are conjugate.]

7. Let G_1 and G_2 be two nontrivial groups. Show that $G_1 \times G_2$ is not a Frobenius group.

8. Let G be a finite group having property $(\mathcal{F}_{\mathrm{top}})$. Show that the number of elements of G of order 2 is either 0 or 1.
[Hint: show that a dihedral group of order > 2 does not have property $(\mathcal{F}_{\mathrm{top}})$. For a direct topological argument, see Milnor [67].]

9. Let G be a nonabelian group of order pq with p, q primes and $p < q$. Let $\rho : G \to \mathrm{GL}(V)$ be an irreducible complex representation of G. Show that, either $\dim V = 1$ and the

elements of order q of G act trivially on V, or $\dim V = p$ and every element of order p of G fixes a nonzero element of V. Conclude that G does not have property $(\mathcal{F})$.

10. Let p and q be two primes (not necessarily distinct). A finite group G is said to have the *pq-property* if every subgroup of G of order pq is cyclic.
Show that property $(\mathcal{F})$ implies the pq-property for every p, q.
[Hint: when p and q are distinct, use exerc.9 above.]
Prove that $\mathrm{SL}_2(\mathbf{F}_\ell)$, ℓ prime, has the pq-property for every p, q if and only if ℓ is a *Fermat prime*[5], i.e., if $\ell = 1 + 2^k$ for some integer $k > 0$.

11. Let s be an element of order 3 of $G = \mathrm{SL}_2(\mathbf{F}_{17})$.
a) Let $\rho : G \to \mathrm{GL}_n(\mathbf{C})$ be a complex linear representation of G. Show that, if $n > 0$, there exists a nonzero element of $\mathbf{C}^n$ which is fixed by $\rho(s)$.
[Hint: one may assume that ρ is irreducible; use the determination of the irreducible characters of G (cf. e.g. ATLAS [16], p.9, or Fulton-Harris [20], §5.2) to compute the eigenvalues of $\rho(s)$ and show that one of them is equal to 1.]
b) Use a) to prove that G does not have property $(\mathcal{F})$.
c) Generalize a) and b) to $\mathrm{SL}_2(\mathbf{F}_\ell)$, with ℓ prime > 5.

[5] The only known Fermat primes are 3, 5, 17, 257 and 65537.

Chapter 7

Transfer

7.1 Definition of Ver : $G^{\mathrm{ab}} \to H^{\mathrm{ab}}$

Let G be a group and let H be a subgroup of G of finite index. Let $X = G/H$, and let $\varphi : X \to G$ be a section. If $g \in G$ and $x \in X$, the elements $\varphi(gx)$ and $g\varphi(x)$ belong to the same class mod H; hence there exists a unique $h^{\varphi}_{g,x} \in H$ such that $g\varphi(x) = \varphi(gx)h^{\varphi}_{g,x}$. Let $\mathrm{Ver}(g) \in H^{\mathrm{ab}}$ be defined by:

$$\mathrm{Ver}(g) = \prod_{x \in X} h^{\varphi}_{g,x} \bmod D(H), \tag{7.1}$$

where the product is computed in $H^{\mathrm{ab}} = H/D(H)$.

Theorem 7.1. *The map* Ver : $G \to H^{\mathrm{ab}}$ *defined above is a homomorphism and it does not depend on the choice of the section* φ.

[This homomorphism is called the **transfer** of G into H^{ab}; one may also view it as a homomorphism $G^{\mathrm{ab}} \to H^{\mathrm{ab}}$. The notation " Ver " comes from the German name "Verlagerung".]

Proof. Let us show first that Ver does not depend on the choice of φ. Let φ' be another section; we have $\varphi'(x) = \varphi(x)\theta(x)$, where θ is a map of X into H. If $g \in G$, we have

$$g\varphi'(x) = g\varphi(x)\theta(x) = \varphi(gx)h^{\varphi}_{g,x}\theta(x) = \varphi'(gx)\theta(gx)^{-1}h^{\varphi}_{s,x}\theta(x),$$

hence $h^{\varphi'}_{g,x} = \theta(gx)^{-1}h^{\varphi}_{g,x}\theta(x)$. When x runs through X, so does gx. Hence :

$$\prod_{x \in X} h^{\varphi'}_{g,x} = \prod_{x \in X} h^{\varphi}_{g,x} \mod D(H),$$

which proves the independence on the choice of φ.

If $g' \in G$, we have

$$gg'\varphi(x) = g\varphi(g'x)h^{\varphi}_{g',x} = \varphi(gg'x)h^{\varphi}_{g,g'x}h^{\varphi}_{g',x};$$

this shows that $h^{\varphi}_{gg',x} = h^{\varphi}_{g,g'x}h^{\varphi}_{g',x}$; by taking the product over all $x \in X$, this gives $\mathrm{Ver}(gg') = \mathrm{Ver}(g)\mathrm{Ver}(g')$, hence Ver is a homomorphism of G into H^{ab}.

Remark. Instead of using sections $\varphi : G/H \to G$, we could have used representative sets mod H, i.e., subsets S of order $(G : H)$ such that $G = SH$. Let $g \in G$. For every $s \in S$ there exists a unique $h_{g,s} \in H$ such that $gs \in Sh_{g,s}$. Equation (7.1) is equivalent to :

$$\mathrm{Ver}(g) = \prod_{s \in S} h_{g,s} \mod D(H). \tag{7.2}$$

Theorem 7.2. *Let $n = (G : H)$ and let $i : H^{\mathrm{ab}} \to G^{\mathrm{ab}}$ be the map deduced from the injection $H \to G$. The composite map $G^{\mathrm{ab}} \xrightarrow{\mathrm{Ver}} H^{\mathrm{ab}} \xrightarrow{i} G^{\mathrm{ab}}$ is $g \mapsto g^n$.*

Proof. Let us keep the notation of the proof of the theorem above. If we make the product (in the abelian group G^{ab}) of the equations $g\varphi(x) = \varphi(gx)h^{\varphi}_{g,x}$, we find $g^n \prod \varphi(x) = \prod \varphi(gx).\mathrm{Ver}(g) \mod D(G)$. Since gx runs through X when x does, we have $\prod \varphi(x) = \prod \varphi(gx) \mod D(G)$, hence $g^n = \mathrm{Ver}(g) \mod D(G)$, as wanted.

Corollary 7.3. *If G is abelian, then* $\mathrm{Ver}(g) = g^n$ *for every $g \in G$.*

Functoriality.

The transfer is obviously *functorial* for isomorphisms. More generally, if σ is a homomorphism from the pair (G, H) to the pair (G', H') which induces a bijection $G/H \to G'/H'$, the diagram

$$\begin{array}{ccc} G^{\mathrm{ab}} & \xrightarrow{\sigma} & G'^{\mathrm{ab}} \\ \Big\downarrow{\scriptstyle \mathrm{Ver}} & & \Big\downarrow{\scriptstyle \mathrm{Ver}} \\ H^{\mathrm{ab}} & \xrightarrow{\sigma} & H'^{\mathrm{ab}} \end{array}$$

is commutative.

Indeed, let $X = G/H = G'/H'$. If $\varphi : X \to G$ is a section of $G \to X$, then the map $\varphi' : X \to G \to G'$ is a section of $G' \to X$. If $g \in G$ and $g' = \sigma(g) \in G'$, then, for every $x \in X$, the image of $h^{\varphi}_{g,x}$ in H' is $h^{\varphi'}_{g',x}$. By taking a product over all $x \in X$, this shows that the image in H'^{ab} of $\mathrm{Ver}(g)$ is $\mathrm{Ver}(g')$.

In particular, if we take $G = G'$, $H = H'$ and $\sigma(x) = zxz^{-1}$ with $z \in N_G(H)$, the commutative diagram reads $z\mathrm{Ver}(x)z^{-1} = \sigma(\mathrm{Ver}(x)) = \mathrm{Ver}(\sigma(x))$. Since we have $\mathrm{Ver}(\sigma(x)) = \mathrm{Ver}(zxz^{-1}) = \mathrm{Ver}(x)$, this shows:

Proposition 7.4. *The image of the homomorphism* $\mathrm{Ver} : G^{\mathrm{ab}} \to H^{\mathrm{ab}}$ *is contained in the set of elements of H^{ab} fixed under conjugation by $N_G(H)$.*

7.2 Computation of the transfer

Let H be a subgroup of G with finite index n and let $X = G/H$. Let $g \in G$, and let C_g be the cyclic subgroup of G generated by g. Then C_g decomposes X into orbits O_α.

Let $f_\alpha = |O_\alpha|$ and let $x_\alpha \in O_\alpha$. We have $g^{f_\alpha} x_\alpha = x_\alpha$. If $z_\alpha \in G$ is a representative of $x_\alpha \in X$, we have

$$g^{f_\alpha} z_\alpha = z_\alpha h_\alpha, \text{ for some } h_\alpha \in H.$$

Theorem 7.5. *We have :*

$$\mathrm{Ver}(g) = \prod_\alpha h_\alpha = \prod_\alpha z_\alpha^{-1} g^{f_\alpha} z_\alpha \mod D(H). \tag{7.3}$$

Proof. Let $\varphi : G/H \to G$ be the section defined by $\varphi(g^i x_\alpha) = g^i z_\alpha$ for $i = 0, 1, \ldots, f_\alpha - 1$. We have $\varphi(gx) = g\varphi(x)$ for every $x \in X$, except when x is equal to $g^{f_\alpha - 1} x_\alpha$ for some α; in that case, $g\varphi(x) = g^{f_\alpha} z_\alpha = g_\alpha h_\alpha = \varphi(gx) h_\alpha$, i.e., the corresponding $h^\varphi_{g,x}$ is h_α. Hence $\mathrm{Ver}(g) = \prod h_\alpha \mod D(H)$.

Proposition 7.6. *Let $\varphi : H \to A$ be a homomorphism of H into an abelian group A. Suppose that $\varphi(h) = \varphi(h')$ whenever $h, h' \in H$ are conjugate in G. Then*

$$\varphi\big(\mathrm{Ver}(h)\big) = \varphi(h)^n, \tag{7.4}$$

for every $h \in H$. [Recall that $n = (G : H)$.]

Proof. Indeed, we have $\varphi\big(\mathrm{Ver}(h)\big) = \prod \varphi(z_\alpha^{-1} h^{f_\alpha} z_\alpha)$. On the other hand, the elements $z_\alpha^{-1} h^{f_\alpha} z_\alpha$ and h^{f_α} are conjugate in G, hence $\varphi(z_\alpha^{-1} h^{f_\alpha} z_\alpha) = \varphi(h^{f_\alpha})$, and we have :

$$\varphi\big(\mathrm{Ver}(h)\big) = \prod \varphi(h^{f_\alpha}) = \prod \varphi(h)^{f_\alpha}.$$

The result then follows from the relation $\sum_\alpha f_\alpha = \sum_\alpha |O_\alpha| = |X| = n$.

Corollary 7.7. *Let C be a subgroup of H having the following property :*

(∗) *If $c \in C$ and $h \in H$ are G-conjugate, they are equal.*

Then $\mathrm{Ver}(c) = c^n \mod D(H)$ *for every $c \in C$.*

Proof. Apply formula (7.3) to $g = c$; this gives $\mathrm{Ver}(c) = \prod h_\alpha$, with $h_\alpha = z_\alpha^{-1} c^{f_\alpha} z_\alpha$. The elements $h_\alpha \in H$ and $c^{f_\alpha} \in C$ are G-conjugate, hence equal because of (∗). We then have $\mathrm{Ver}(c) = c^{\sum f_\alpha} = c^n \mod D(H)$.

Corollary 7.8. *Assume that, if two elements of H are conjugate in G, they are equal. Then :*
(1) $\mathrm{Ver}(h) = h^n$ *for every $h \in H$.*
(2) *Assume that $|H|$ and $(G : H)$ are relatively prime. Let $N = \mathrm{Ker}(\mathrm{Ver} : G \to H)$. Then N is a normal complement of H, i.e., G is the semidirect product of H and N.*

Proof. Note that the hypothesis on H implies that H is abelian, so that the transfer $\mathrm{Ver} : G \to H^{\mathrm{ab}}$ does map G into H. Assertion (1) then follows from cor.7.7; under the assumption of (2), it implies that the composite map $H \to G \overset{\mathrm{Ver}}{\to} H$ is an isomorphism, which is equivalent to G being the semidirect product of H and N.

Corollary 7.9. *Assume that H is contained in the center of G and that $|H|$ and $|G/H|$ are relatively prime. Then $G \simeq H \times G/H$.*

Proof. This follows from cor.7.8, since N centralizes H.

Remark. Corollary 7.9 is a special case of Zassenhaus's th.4.20; its first proof, by Frobenius ([19], n° 63), used character theory; the proof given here is due to Schur, [34], see the historical note of §7.8.

Theorem 7.10. *Assume that H is abelian and normal in G. Let $g \in G$; let f be the smallest integer > 0 such that $g^f \in H$; let C_g be the cyclic subgroup generated by g. Then :*

$$\mathrm{Ver}(g) = \prod_{\gamma \in G/C_g H} \gamma g^f \gamma^{-1}. \tag{7.5}$$

[Note that, if $\gamma \in G$, then $\gamma g^f \gamma^{-1}$ depends only on the left coset of γ mod $C_g H$; hence the product in equation (7.5) makes sense.]

Proof. Let γ_α be a set of representatives of $G/C_g H$, and let x_α be the image of γ_α^{-1} in $X = G/H$. The orbits of C_g in X are the $C_g x_\alpha$. We may then apply formula (7.3) with $z_\alpha = \gamma_\alpha^{-1}, f_\alpha = f$ and $h_\alpha = \gamma_\alpha g^f \gamma_\alpha^{-1}$; we obtain (7.5).

Corollary 7.11. *If $h \in H$, then* $\mathrm{Ver}(h) = \prod_{\gamma \in G/H} \gamma h \gamma^{-1}$.

Proof. This is the special case $f = 1$.

7.3 A two-century-old example of transfer: Gauss lemma

Let p be a prime number $\neq 2$.

Let $G = \mathbf{F}_p^\times$ and let $H = \{\pm 1\}$. The index of H in G is $(p-1)/2$; the transfer $\mathrm{Ver} : G \to H$ is thus given by $\mathrm{Ver}(x) = x^{(p-1)/2}$, which is the **Legendre symbol** $\left(\frac{x}{p}\right)$: it is 1 if x is a square, and -1 if not. We may thus compute $\left(\frac{x}{p}\right)$ by using the recipe of §7.1. This means choosing first a representative set S of $X = G/H$, for instance $S = \{1, 2, \ldots, (p-1)/2\}$; for $x \in G$ and $s \in S$, define $\varepsilon(x, s) = \pm 1$ as being 1 if $xs \in S$ and -1 if $xs \notin S$. Then:

$$\left(\frac{x}{p}\right) = \prod_{s \in S} \varepsilon(x, s). \tag{7.6}$$

This is *Gauss lemma*; it is used in some of the proofs of the quadratic reciprocity law. Here is a simple example:

Computation of $\left(\frac{2}{p}\right)$. Let $m = (p-1)/2$, so that $S = \{1, \ldots, m\}$. If $s \in S$ we have $\varepsilon(2, s) = -1$ if and only if $m/2 < s \leqslant m$. If m is even, the number of such s is $m/2$; this shows that $\left(\frac{2}{p}\right)$ is equal to 1 if and only if $m/2$ is even, i.e., if $p \equiv 1 \pmod 8$. If m is odd, the number of such s is $(m+1)/2$, hence $\left(\frac{2}{p}\right)$ is equal to 1 if and only $(m+1)/2$ is even, i.e., if $p \equiv -1 \pmod 8$. This gives :

$$\left(\frac{2}{p}\right) = 1 \iff p \equiv \pm 1 \pmod 8 \quad \text{hence} \quad \left(\frac{2}{p}\right) = -1 \iff p \equiv \pm 5 \pmod 8.$$

7.4 An application of transfer to infinite groups

Proposition 7.12. *If G is a torsion-free group with a finite index subgroup H isomorphic to $\mathbf{Z}$, then G is isomorphic to $\mathbf{Z}$.*

[An element of a group is called a *torsion element* if its order is finite; a group is called *torsion-free* if it has no torsion element $\neq 1$.]

Proof. After replacing H by the intersection of its conjugates, we may assume that H is normal in G. The group G acts on H by conjugation and this action yields a group homomorphism $\varepsilon : G \to \mathrm{Aut}(H) = \{\pm 1\}$. There are two cases:

(a) $\varepsilon = 1$, i.e., H is contained in the center of G. Let $v : G \to H$ be the transfer map. By cor.7.8, we have $v(h) = h^n$ for every $h \in H$, where $n = (G : H)$. Since H is isomorphic to $\mathbf{Z}$, this shows that the restriction of v to H is injective; if $N = \mathrm{Ker}(v)$, we have $N \cap H = 1$, hence N is finite. Since G is torsion-free, this implies $N = 1$, i.e., v is injective. Hence G is isomorphic to a nonzero subgroup of $\mathbf{Z}$, hence it is isomorphic to $\mathbf{Z}$.

(b) $\varepsilon \neq 1$. Let G' be its kernel. By a), applied to G', we have $G' \simeq \mathbf{Z}$. Let $x \in G - G'$; the action of x on G' by conjugation is nontrivial (since it is nontrivial on H), hence it is $y \mapsto y^{-1}$. We have $x^2 \in G'$ since G/G' has order 2. Hence $x.x^2.x^{-1} = x^{-2}$, i.e., $x^4 = 1$; this is impossible since G is torsion free and $x \neq 1$. Hence case (b) does not occur.

Remarks.

1) A similar result holds for free nonabelian groups, cf. Stallings [74] and Swan [76]. The proof uses "geometric group theory".

2) The theorem does not exend to free abelian groups of higher rank: for every $r > 1$, there exist nonabelian torsion-free groups which contain a subgroup of finite index isomorphic to $\mathbf{Z}^r$, see exerc.13. Such groups are called *Bieberbach groups*; they are useful for the classification of compact flat Riemannian manifolds, cf. Wolf [40], chap.3.

7.5 Transfer applied to Sylow subgroups

From now on, we assume that G is finite.

Theorem 7.13. *Let H be a p-Sylow subgroup of G and let $\varphi : H \to A$ be a homomorphism with values in a finite abelian p-group A. Then :*

(1) φ extends to a homomorphism of G into A if and only if, for all $h, h' \in H$ conjugate in G, we have $\varphi(h) = \varphi(h')$.

(2) If an extension of φ to G exists, it is unique, and it is given by $g \mapsto \varphi(\mathrm{Ver}(g))^{1/n}$, where $n = (G : H)$ [this makes sense since n and p are relatively prime].

Proof of (1). The condition is necessary because, if $\widetilde{\varphi}$ is an extension of φ to G, then, for $h \in H$ and $g \in G$ with $g^{-1}hg \in H$, we have

$$\varphi(g^{-1}hg) = \widetilde{\varphi}(g)^{-1}\varphi(h)\widetilde{\varphi}(g) = \varphi(h),$$

since A is abelian.
The condition is sufficient: since p and the index n are relatively prime, and since A is a p-group, $\varphi(\mathrm{Ver}(g))^{1/n}$ makes sense (for all $a \in A$, there exists a unique $b \in A$ such that $b^n = a$) and the map $g \mapsto \varphi(\mathrm{Ver}(g))^{\frac{1}{n}}$ is an extension of φ, thanks to prop.7.6.

Proof of (2). Let $\widetilde{\varphi}$ and $\widetilde{\varphi}'$ be two extensions of φ to G and let B be the group of all $g \in G$ such that $\widetilde{\varphi}(g) = \widetilde{\varphi}'(g)$. The group B contains H by assumption; it also contains the p'-Sylow subgroups of G with $p' \neq p$ since both $\widetilde{\varphi}$ and $\widetilde{\varphi}'$ take the value 1 on such groups. This implies $B = G$ (for instance because the index of B is divisible neither by p nor by any prime $p' \neq p$, hence is equal to 1).

Theorem 7.14. *Let H be an abelian p-Sylow subgroup of G and let N be its normalizer in G. Then the image of* Ver : $G^{\mathrm{ab}} \to H^{\mathrm{ab}} = H$ *is* $H^N = H \cap Z(N)$.

Proof. The group Im(Ver) is contained in $H^N = \{h \in H |\ xhx^{-1} = h,\ \text{for all } x \in N\}$, cf. prop.7.4.
Let us show the opposite inclusion. Let $C = H^N$. If $c \in C$ and $h \in H$ are G-conjugate, then they are N-conjugate (th.2.17); hence they are equal since c is fixed under N-conjugation. If $c \in C$, by cor.7.7, we have $\mathrm{Ver}(c) = c^n$. Since n is prime to p, the map $c \mapsto c^n$ is an automorphism of C. This shows that C is contained in Im(Ver).

Theorem 7.15. *Let H be a p-Sylow subgroup of G. Suppose that H is nontrivial abelian and that G has no cyclic quotient of order p. Let N be the normalizer of H in G. Then :*

(1) $H^N = 1$, *where H^N is the set of elements of H fixed under N-conjugation.*

(2) *There exists a prime number ℓ which divides both $(N : H)$ and $\prod_{i=1}^r (p^i - 1)$, where r is the rank of the p-group H.*

Proof of (1). Theorem 7.14 shows that Ver : $G \to H^N$ is surjective. If $H^N \neq 1$, this implies that G has a quotient that is cyclic of order p, which contradicts the assumption made on G.

Proof of (2). Let C be the image of N in $\mathrm{Aut}(H)$; this group is a quotient of N/H, hence its order is prime to p. By cor.3.30, $|C|$ divides $\prod_{i=1}^r (p^i - 1)$. By (1), we have $|C| > 1$. We then take for ℓ a prime divisor of $|C|$.

Corollary 7.16. *We have $N_G(H) \neq H$.*

Proof. If $N_G(H) = H$, we have $H^N = H$, contrary to (1).

Corollary 7.17. *If $p = 2$, the subgroup H is not cyclic.*

Proof. Indeed, we have $r \geqslant 2$ by th.7.15 [for a transfer-free proof, see exerc.11 of chap.2].

7.6 Application: groups of odd order < 2000

We prove a baby case of the Feit-Thompson theorem:

Proposition 7.18. *A group of odd order* < 2000 *is solvable.*

Equivalently:

Corollary 7.19. *A simple group of odd order* < 2000 *is cyclic.*

Proof. Let G be a nonsolvable group of odd order $N < 2000$. Write N as $\prod p_1^{m_1} \cdots p_n^{m_n}$, where the p_i are distinct primes and we have $1 < p_1^{m_1} < p_2^{m_2} < \cdots < p_n^{m_n}$. According to Burnside's theorem (cf. chap.8, th.8.62), we have $n \geqslant 3$, hence $p_1^{m_1} < 2000^{1/3} < 13$, which implies that $p_1^{m_1}$ is equal to 3, 5, 7, 9 or 11.
Note that $p_i^{m_i}$ cannot be 3, 5 or 9 : indeed, if it were, th.7.15 applied with $p = p_i$ would imply the existence of a prime ℓ dividing both N and one of the number 2, 4 or 16; this is impossible since $|G|$ is odd. This shows that $p_1^{m_1} = 7$ or 11.
If $p_1^{m_1} = 7$, th.7.15 shows that 3 divides N. The corresponding factor of N cannot be 3 or 9; hence it is at least 27, and the other factors of N are $< 2000/7.27 < 7$, which is impossible.
If $p_1^{m_1} = 11$, a similar argument shows that 5 divides N and that the other factors of N are $< 2000/11.25 < 7$, which is impossible.
Conclusion: such a group G does not exist.

7.7 Application: simple groups of order $\leqslant 200$

We prove a baby case of CFSG:

Theorem 7.20. *Let G be a nonabelian simple group of order* $\leqslant 200$. *The order of G is either* 60 *or* 168.

Lemma 7.21. *Let G be a nonabelian simple group, and let A be a proper subgroup of G. Then* $(G:A) \geqslant 5$; *moreover* $(G:A) = 5$ *is impossible if* $|G| > 60$.

Proof of the lemma. If $n = (G:A)$ is > 1, the action of G on G/A gives a nontrivial homomorphism $G \to \mathcal{S}_n$, which is injective because G is simple. This is impossible if $n = 2, 3$ or 4 since $\mathcal{S}_n$ is solvable. When $n = 5$, the image of G in $\mathcal{S}_5$ is contained in $\mathcal{A}_5$ (otherwise G would have a quotient of order 2); hence $|G| \leqslant 60$.

Proof of theorem 7.20. Let H be a 2-Sylow subgroup of G. By prop.7.18 , H is nontrivial, and by cor.7.17 it is not cyclic, hence its order is $\geqslant 4$. We thus have two cases:

a) The case $|H| = 4$.
The group H is elementary abelian of type $(2,2)$, hence $\mathrm{Aut}(H) \simeq \mathcal{S}_3$. Let N be the normalizer of H in G. By th.7.15, the homomorphism $N/H \to \mathrm{Aut}(H)$ is not trivial; since N/H has odd order, its image in $\mathrm{Aut}(H)$ has order 3. Hence $|G|$ is divisible by 3

and by 4; let us write it as $|G| = 4.3.q$, with q odd; we have $q \leqslant 200/12 < 17$; moreover, by Burnside's theorem (chap.8, th.8.62), q is divisible by at least one prime > 3. There are thus five possibilities : $q = 5, 7, 11, 13, 15$. The case $q = 5$ gives $|G| = 60$. Let us show that the other cases are impossible:

a_1) *The subcases* $q = 7, 11, 13$.
Let S be a q-Sylow subgroup of G, and let N_S be its normalizer. The index $(G : N_S)$ is a divisor of 12, since N_S contains S; it is not equal to 1 since G is simple; it is not equal to 12 by th.7.15, applied to the prime number q; it is > 5 by lemma 7.21. Hence we have $(G : N_S) = 6$. But this is impossible, because $(G : N_S)$ is the number of q-Sylow subgroups of G, hence is $\equiv 1 \pmod{q}$ and $q = 7, 11$ or 13.

a_2) *The subcase* $q = 15$.
Let S be a 5-Sylow subgroup of G, and let N_S be its normalizer. We use the same arguments as in a_1) : the index $(G : N_S)$ is a divisor of 36; it is not equal to 1 because G is simple, and it is not equal to 36 by th.7.15; it is > 5 by lemma 7.21. Hence $(G : N_S) = 6, 9$ or 12. By Sylow's second theorem, it is $\equiv 1 \pmod{5}$). This leaves the only possibility $(G : N_S) = 6$. But in that case, the action of G on G/N_S gives an embedding of G into $\mathcal{A}_6$; since $|G| = 180$ and $\mathcal{A}_6 = 360$, the index of G in $\mathcal{A}_6 = 360$ is 2, which is impossible (either because every subgroup of index 2 is normal, or by lemma 7.21 applied to $\mathcal{A}_6$).

b) *The case* $|H| \geqslant 8$.
We have $(G : H) \leqslant 200/8 = 25$. Since $(G : H)$ is divisible by at least two distinct primes > 2, this leaves only the two possibilities $(G : H) = 15$ and $(G : H) = 21$, with $|H| = 8$.. The second one gives $|G| = 168$. Let us show that the first one, $|G| = 120$, is impossible. The argument is the same as in a_2):
Let S be a 5-Sylow subgroup of G and let N_S be its normalizer. The index $(G : N_S)$ is a divisor of 24; it is not equal to 1 because G is simple, and it is not equal to 24 by th.7.15; it is > 5 by lemma 7.21; by Sylow's second theorem it is $\equiv 1 \pmod{5}$. Hence we have $(G : N_S) = 6$, and we thus get an embedding of G into $\mathcal{A}_6$; this gives a subgroup of $\mathcal{A}_6$ of index 3, which is impossible by lemma 7.21 applied to $\mathcal{A}_6$.

Theorem 7.22. *A simple group of order* 60 *is isomorphic to* $\mathcal{A}_5$.

Proof. Let G be such a group. It is nonabelian since 60 is not a prime number. Let H be a 2-Sylow subgroup of G and let N be its normalizer. We have seen in part a) of the proof of th.7.20 that the order of N is divisible by 12, hence is equal to 12, otherwise N would be equal to G. We have $(G : N) = 5$. The action of G on G/N gives an embedding of G into $\mathcal{A}_5$; since these groups have the same order, that embedding is an isomorphism.

Theorem 7.23. *A simple group of order* 168 *is isomorphic to* $\mathrm{PSL}_2(\mathbf{F}_7)$.

Proof. Let G be such a group, let U be a 7-Sylow subgroup of G and let B be its normalizer. Then $(G : B)$ divides 8.3 and $(G : B) \equiv 1 \pmod{7}$. Since $B \neq G$, we have $(G : B) = 8$. Hence, $|B| = 21$. By th.7.15, the homomorphism $B/U \to \mathrm{Aut}(U) = \mathbf{F}_7^\times$ is

nontrivial; hence it gives an isomorphism of B/U onto the subgroup of order 3 of $\mathbf{F}_7^\times$, which is $\{1,2,4\}$.

Let T be a 3-Sylow subgroup of B, and let t be the unique element of T whose image in $\mathbf{F}_7^\times$ is 2; we have $tut^{-1} = u^2$ for every $u \in U$.

Let $X = G/B$ be the set of the 7-Sylow subgroups of G. We have $|X| = 8$. Denote by ∞ the point of X corresponding to U; its stabilizer is B. The action of U on $X - \{\infty\}$ is free and transitive (otherwise, U would act trivially on X). The group T acts on $X - \{\infty\}$; since that set has 7 elements, T fixes one of them; call x_0 such an element. Choose a generator u of U. We have:

$$X = \{x_0, ux_0, u^2x_0, \ldots, u^6x_0, \infty\}.$$

We now identify X with the projective line $\mathbf{P} = \mathbf{P}_1(\mathbf{F}_7) = \mathbf{F}_7 \cup \{\infty\}$ by $u^ix_0 \mapsto i$ and $\infty \mapsto \infty$. We may thus view G as a group of permutations of $\mathbf{P}$, and we are going to show that *G is the group* $\mathrm{PSL}_2(\mathbf{F}_7)$ *of fractional linear transformations* $i \mapsto (ai+b)/(c+id)$, *with* $a,b,c,d \in \mathbf{F}_7$ *and* $ad-bc$ *a nonzero square.*

Note that u is indeed a fractional linear transformation, namely $i \mapsto i+1$.

As for t, we have $t(0) = 0$ and $tu(i) = u^2t(i)$ for every i, i.e., $t(i+1) = 2 + t(i)$. By induction on i, this gives $t(i) = t(1) + 2i - 2$, and $t(0) = 0$ implies $t(1) = 2$, so that $t(i) = 2i$ for every i. Hence t acts on P by the homothety $i \mapsto 2i$. In particular, the orbits of T on $\mathbf{P}$ are: $\{0\}$, $\{\infty\}$, $\{1,2,4\}$, $\{3,5,6\}$.

Let N be the normalizer of T. Theorem 7.15 shows that N acts nontrivially on T; since $\mathrm{Aut}(T) = \{1,-1\}$, there exists an element $w \in N$ which belongs to the 2-Sylow subgroup of N and is such that $wtw^{-1} = t^{-1}$. This property implies that w permutes the four orbits of T. In particular, w stabilizes $\{0,\infty\}$. It cannot fix these two points, since the stabilizer of an element of P had order 21, which is odd. Hence it permutes $\{0\}$ and $\{\infty\}$. Its square w^2 fixes $\{0\}$ and $\{\infty\}$; hence $w^2 = 1$, by the same argument as above.

Since w has no fixed point, it does not stabilize the set $\{1,2,4\}$; hence it maps it onto $\{3,5,6\}$. Let $\lambda = w(1)$; we have $\lambda = 3, 5$ or 6. The relation $wt = t^{-1}w$ shows that $w(2i) = 4w(i)$ for every i, hence $w(2) = 4\lambda, w(4) = 2\lambda$. Since $w^2 = 1$, we have $w(\lambda) = 1, w(2\lambda) = 4\lambda, w(4\lambda) = 2\lambda$. These formulas can be summed up as : $w(i) = \lambda/i$ for every $i \neq 0, \infty$.

This shows that w is also a fractional linear transformation.
We may write it as $i \mapsto (ai+b)/(ci+d)$ with $a = d = 0, b = \lambda, c = 1$, so that $ad - bc = -\lambda$, which is a square; hence w belongs to $\mathrm{PSL}_2(\mathbf{F}_7)$. Let now G' be the subgroup of G generated by B and w. The order of G' is divisible by 2.3.7; its index is thus $1, 2$ or 4. By lemma 7.21, this index cannot be 2, nor 4; hence it is equal to 1, i.e., $G' = G$. Since G' is contained in $\mathrm{PSL}_2(\mathbf{F}_7)$, which has also order 168, these two groups are equal, and we have $G = \mathrm{PSL}_2(\mathbf{F}_7)$, as wanted.

Remark. The above proof looks more natural in terms of algebraic groups: with standard terminology, B is a Borel subgroup, U is its unipotent radical, T is a maximal torus of B, and $N/T \simeq \{1, w\}$ is the Weyl group; this explains our choice of letters.

7.8 The use of transfer outside group theory

This section is intended for readers who want to see how the transfer map occurs in several questions of algebraic number theory, algebra, and topology. We assume acquaintance with the basic definitions of these topics. The proofs of 7.8.3 and 7.8.4 amount to using equation (7.3) of th.7.5; they are straightforward. As for 7.8.1 and 7.8.2 (originally due to Artin and to Chevalley), they are special cases of a general result of Artin-Tate on *class formations*, see Artin-Tate [1], chap.XIV, §5, th.5 a), and also [35], chap. XI, §3.

7.8.1. Abelian extensions of number fields.

Let $E \supset L \supset K$ be three number fields. Assume that E is a Galois extension of K; let $G = \mathrm{Gal}(E/K)$ and $H = \mathrm{Gal}(E/L)$. Denote by C_K and C_L the *idèle class groups* of K and L. The *Artin map* for K (a.k.a. *the reciprocity map*) is a surjective homomorphism $C_K \to G^{\mathrm{ab}}$, cf. Lang [31], chap. X and Cassels-Fröhlich [14], chap. VII; similarly we have $C_L \to H^{\mathrm{ab}}$. The commutative diagrams below give the relations between these maps [in these diagrams the arrows "func" denote the homomorphisms defined by functoriality; for instance func : $C_K \to C_L$ comes from the natural embedding of the idèles of K into the idèles of L] :

$$\begin{array}{ccc} C_K & \longrightarrow & G^{\mathrm{ab}} \\ \text{func}\downarrow & & \downarrow \text{Ver} \\ C_L & \longrightarrow & H^{\mathrm{ab}} \end{array} \qquad\qquad \begin{array}{ccc} C_K & \longrightarrow & G^{\mathrm{ab}} \\ \text{norm}\uparrow & & \uparrow \text{func} \\ C_L & \longrightarrow & H^{\mathrm{ab}}. \end{array}$$

Note that here, and also in 7.8.2, the transfer on the group level corresponds to the functoriality map on the field level; that is not the case in 7.8.3 and 7.8.4.

7.8.2. Abelian extensions of local fields.

We keep the same notation (E, L, K) as above, except that now K is a *local field*, i.e., a finite extension of either $\mathbf{Q}_p$ or $\mathbf{F}_p((t))$. The local reciprocity map is a surjective homomorphism $K^\times \to G^{\mathrm{ab}}$, cf. [35], chap. XIII and Cassels-Fröhlich [14], chap. VI, §2.2; similarly we have $L^\times \to H^{\mathrm{ab}}$. These maps are related by the following commutative diagrams ([14], chap. VI, §2.4) :

$$\begin{array}{ccc} K^\times & \longrightarrow & G^{\mathrm{ab}} \\ \text{func}\downarrow & & \downarrow \text{Ver} \\ L^\times & \longrightarrow & H^{\mathrm{ab}} \end{array} \qquad\qquad \begin{array}{ccc} K^\times & \longrightarrow & G^{\mathrm{ab}} \\ \text{norm}\uparrow & & \uparrow \text{func} \\ L^\times & \longrightarrow & H^{\mathrm{ab}}. \end{array}$$

7.8.3. Kummer theory.

Let $E \supset L \supset K$ be three fields; as in the first example, we assume that E is a finite Galois extension of K and we put $G = \mathrm{Gal}(E/K)$ and $H = \mathrm{Gal}(E/L)$. Let n be an integer $\geqslant 1$, and let μ_n be the subgroup of $K^\times$ made up of the n-th roots of unity; assume $|\mu_n| = n$. Kummer theory (cf. Bourbaki [4], V.11.8 and Lang [29], VI, §8) gives[1] an embedding $\mathrm{Hom}(G^{\mathrm{ab}}, \mu_n) \longrightarrow K^\times/K^{\times n}$. Similarly, we have $\mathrm{Hom}(H^{\mathrm{ab}}, \mu_n) \longrightarrow L^\times/L^{\times n}$. The following diagrams are commutative:

$$\begin{array}{ccc} \mathrm{Hom}(G^{\mathrm{ab}}, \mu_n) & \longrightarrow & K^\times/K^{\times n} \\ \mathrm{Ver}_n \uparrow & & \uparrow \mathrm{norm} \\ \mathrm{Hom}(H^{\mathrm{ab}}, \mu_n) & \longrightarrow & L^\times/L^{\times n} \end{array} \qquad \begin{array}{ccc} \mathrm{Hom}(G^{\mathrm{ab}}, \mu_n) & \longrightarrow & K^\times/K^{\times n} \\ \mathrm{func} \downarrow & & \downarrow \mathrm{func} \\ \mathrm{Hom}(H^{\mathrm{ab}}, \mu_n) & \longrightarrow & L^\times/L^{\times n}. \end{array}$$

[In the left diagram, Ver_n denotes the map $f \mapsto f \circ \mathrm{Ver}$ of $\mathrm{Hom}(H^{\mathrm{ab}}, \mu_n)$ into $\mathrm{Hom}(G^{\mathrm{ab}}, \mu_n)$. One may view it as a *corestriction map* $\mathrm{cor} : H^1(H, \mu_n) \to H^1(G, \mu_n)$, cf. Remark at the end of §4.2.]

7.8.4. Fundamental groups and covering spaces.

Let $f : Y \to X$ be a finite covering of topological spaces, of degree $n \geqslant 1$; suppose that X and Y are arcwise connected; let y be a point of Y, and put $x = f(y) \in X$. Let $\pi_1(X, x)$ denote the fundamental group of X at the base point x, and define similarly $\pi_1(Y, y)$. The natural map $\pi_1(Y, y) \to \pi_1(X, x)$ is injective; we may thus view $\pi_1(Y, y)$ as a subgroup of $\pi_1(X, x)$; its index is n. [Reference: Hatcher [23], chap.1.]

Let $H_1(X)$ be the first homology group of X with coefficients in $\mathbf{Z}$ (in singular homology theory, cf. Hatcher, *loc.cit.*, chap.2); define similarly $H_1(Y)$. We have natural isomorphisms $H_1(X) \simeq \pi_1(X, x)^{\mathrm{ab}}$ and $H_1(Y) \simeq \pi_1(Y, y)^{\mathrm{ab}}$.

There is an *inverse image map* $f^* : H_1(X) \to H_1(Y)$ defined as follows: if s is a singular 1-simplex of X (i.e., a continuous map $[0, 1] \to X$), then s has n distinct liftings to Y; let $\tilde{s}$ be the sum of these liftings; the map $s \mapsto \tilde{s}$ extends by linearity to a map of the 1-chains of X into the 1-chains of Y; the corresponding map on homology is f^*.
These maps are related by the commutative diagrams:

$$\begin{array}{ccc} H_1(X) & \simeq & \pi_1(X, x)^{\mathrm{ab}} \\ f^* \downarrow & & \downarrow \mathrm{Ver} \\ H_1(Y) & \simeq & \pi_1(Y, y)^{\mathrm{ab}} \end{array} \qquad \begin{array}{ccc} H_1(X) & \simeq & \pi_1(X, x)^{\mathrm{ab}} \\ \mathrm{func} \uparrow & & \uparrow \mathrm{func} \\ H_1(Y) & \simeq & \pi_1(Y, y)^{\mathrm{ab}}. \end{array}$$

[1] If $\varphi \in \mathrm{Hom}(G, \mu_n)$, there exists $x \in E^\times$ such that $\varphi(g) = x^{-1}g(x)$ for every $g \in G$; one has $x^n \in K^\times$, and one associates to φ the image of x^n in $K^\times/K^{\times n}$; this gives an embedding of $\mathrm{Hom}(G^{\mathrm{ab}}, \mu_n)$ into $K^\times/K^{\times n}$.

Historical note.

It seems that the map we now call transfer occurred for the first time in 1902, in Schur [34], n° 3. In this paper, Schur constructs that map, without giving it a name, and proves its main elementary properties. He uses it to prove cor.7.9, namely:

If $1 \to A \to G \to B \to 1$ *is a central extension, and if* A, B *are finite of relatively prime orders, then* $G \simeq A \times B$.

In 1929, Artin (cf. [42]) related that map (applied to Galois groups) to the natural map between ideals of a small field and a larger field (this is a special case of the commutativity of diagram 7.8.1). His goal was the following statement (called the *Hauptidealsatz*, i.e., the *Principal Ideal theorem*), answering a question of Hilbert :

(H) - *Let* K *be a number field and let* L *be its Hilbert class field (maximal abelian extension of* K *which is unramified at every place - including the archimedean ones); let* A_K *and* A_L *be their rings of algebraic integers. Then, if* $\mathbf{a}$ *is an ideal of* A_K*, the ideal* $\mathbf{a}A_L$ *of* A_L *is a principal ideal.*

He showed that this number-theoretic statement is a consequence of the following group-theoretic one:

(T) - *Let* G *be a finite group, and let* $H = D(G)$ *be its derived group. Then the transfer map* $\mathrm{Ver} : G^{\mathrm{ab}} \to H^{\mathrm{ab}}$ *is trivial, i.e.,*$\mathrm{Ver}(g) = 1$ *for every* $g \in G$.

A proof of (T) was soon found by Furtwängler; it is reproduced in Hasse's *Bericht* [59], §28; simpler proofs were given later, especially by Witt: see Artin-Tate [1], chap.XIII, §4. As for the name "Verlagerung" , it was coined by Hasse in [59], §27.

Around 1950, it was realized by several algebraists and topologists such as Eilenberg-Mac Lane and Eckmann, that the transfer is a special case of the restriction and corestriction maps in group cohomology and group homology, see e.g., Cartan-Eilenberg [13], Brown [11], Lang [30].

7.9 Exercises

1. (*Deviations and invariants.*) Let A be a commutative group, acting freely (by a *right action*) on a set Y. Let $X = Y/A$; assume that X is finite; denote by π the projection $Y \to X$.
   Let $\varphi, \varphi' : X \to Y$ be two sections of π; let $\varepsilon : X \to A$ be such that $\varphi'(x) = \varphi(x)\varepsilon(x)$ for every $x \in X$. Let $d(\varphi', \varphi) \in A$ be defined by

$$d(\varphi', \varphi) = \prod_{x \in X} \varepsilon(x).$$

   a) If $\varphi, \varphi', \varphi''$ are three sections of π, show that $d(\varphi'', \varphi) = d(\varphi'', \varphi')d(\varphi', \varphi)$.
   b) Let $\mathrm{Aut}_A(Y)$ be the group of automorphisms of the A-set Y. If $g \in \mathrm{Aut}_A(Y)$, denote by g_X the corresponding element of $\mathcal{S}_X$; if φ is a section of π, then $g\varphi = g \circ \varphi \circ g_X^{-1}$ is a section of π. Show that, if φ and φ' are two sections, then $d(g\varphi', g\varphi) = d(\varphi', \varphi)$.
   c) Use a) and b) to show that $v(g) = d(g\varphi, \varphi)$ is independent of the choice of φ. Show

that $v : \mathrm{Aut}_A(Y) \to A$ is a homomorphism.
d) Let C_g be the cyclic group generated by g. The action of C_g on X gives a partition of X into orbits O_α; for each α, chooses $x_\alpha \in O_\alpha$ and $y_\alpha \in Y$ with $\pi(y_\alpha) = x_\alpha$. Let $f_\alpha = |O_\alpha|$; let a_α be the unique element of A such that $g^{f_\alpha} y_\alpha = y_\alpha a_\alpha$. Show that

$$v(g) = \prod_\alpha a_\alpha.$$

2. (*Another definition of transfer.*) Let G be a group, and let H be a subgroup of finite index of G. Let $A = H^{\mathrm{ab}} = H/D(H)$. Let $Y = G/D(H)$. There is a natural right action of A on Y; that action is free. The left action of G on Y commutes with the action of A, hence gives a homomorphism $G \to \mathrm{Aut}_A(Y)$. By exerc.1, we have a homomorphism $v : \mathrm{Aut}_A(Y) \to A$. Show that $G \to \mathrm{Aut}_A(Y) \xrightarrow{v} A$ is the transfer map $\mathrm{Ver} : G \to A = H^{\mathrm{ab}}$.

3. (*Transitivity of transfer.*) Show that, if $G \supset H \supset K$, with $(G : K)$ finite, then the transfer $\mathrm{Ver} : G^{\mathrm{ab}} \to K^{\mathrm{ab}}$ is the composite of $\mathrm{Ver} : G^{\mathrm{ab}} \to H^{\mathrm{ab}}$ and $\mathrm{Ver} : H^{\mathrm{ab}} \to K^{\mathrm{ab}}$.

4. (*Restriction of the transfer to a subgroup.*) Let H be a subgroup of finite index of a group G, and let K be a subgroup of G. Let Σ be a representative set of the double cosets KxH (i.e., G is the disjoint union of the KsH, for $s \in \Sigma$). If $s \in \Sigma$, let $K_s = K \cap sHs^{-1}$ and let $H_s = s^{-1}Ks \cap H = s^{-1}K_s s$. Show that $K^{\mathrm{ab}} \to G^{\mathrm{ab}} \xrightarrow{\mathrm{Ver}} H^{\mathrm{ab}}$ is equal to the product, for all $s \in \Sigma$, of the homomorphisms $K^{\mathrm{ab}} \xrightarrow{\mathrm{Ver}} K_s^{\mathrm{ab}} \xrightarrow{\sim} H_s^{\mathrm{ab}} \to H^{\mathrm{ab}}$, where $K_s^{\mathrm{ab}} \xrightarrow{\sim} H_s^{\mathrm{ab}}$ is the isomorphism induced by $\mathrm{int}_{s^{-1}}$.
When K is the cyclic group generated by an element g of G, show that this formula is the same as (7.3).

5. Let H be a subgroup of finite index n of a group G and let $g \in Z(G)$. Show that $\mathrm{Ver}(g) = g^n \bmod D(H)$. (This makes sense since g^n belongs to H, cf. chap.1, exerc.3.) [Hint: let m be the smallest integer > 0 such that $g^m \in H$. Use formula (7.3) to compute $\mathrm{Ver}(g)$, and observe that all the $z_\alpha^{-1} g^{f_\alpha} z_\alpha$ of that formula are equal to g^m; conclude by showing that the number of such terms is n/m.]

6. Let E be a finite group having a p-Sylow subgroup H of index n, which splits as $A \times B$, with $A \subset Z(E)$. Show that there exists a normal subgroup N of E such that $E = A \times N$. [Hint: Let $\phi : E \to A$ be the composite map $E \xrightarrow{\mathrm{Ver}} H^{\mathrm{ab}} \to A$. Use exerc.5 to show that $\phi(a) = a^n$ for $a \in A$. Take $N = \mathrm{Ker}\,\phi$.]

7. (*A case where a central extension which splits over a Sylow subgroup splits over the whole group.*)
Let $1 \to A \to E \to G \to 1$ be a central extension of a finite group G by a finite abelian p-group A. Let S be a p-Sylow subgroup of G. Assume that the extension splits over S, i.e., that one can lift S to a subgroup of E.
a) Show that the extension E splits, hence that $E \simeq A \times G$.
[Hint: the inverse image H of S in E is $A \times B$, where B is a lifting of S. Apply exerc.6.]
b) Deduce from a) that the restriction map $H^2(G, A) \to H^2(S, A)$ is injective.

8. (*Burnside.*) Let S be a p-Sylow subgroup of a finite group G. Suppose that S is contained in the center of $N_G(S)$. Show that G is p-nilpotent (cf. exerc.3 of chap.3).
[Hint: apply th.7.14 with $H = S$.]

9. (*Groups which are finite modulo their center.*) Let G be a group and let $\Gamma = G/Z(G)$.
a) Let γ_1, γ_2 be two elements of Γ, and let g_1, g_2 be two representatives of γ_1, γ_2 in G. Show that the commutator (g_1, g_2) depends only on γ_1, γ_2. This gives a map $c : \Gamma \times \Gamma \to D(G)$. Show that the image of c generates $D(G)$.
b) Assume that Γ is finite, and let n be its order.
Show that $D(G)$ and $D(G) \cap Z(G)$ are finitely generated.
Show that $g \in D(G) \cap Z(G)$ implies $g^n = 1$.
[Hint: use the transfert map Ver : $G^{\mathrm{ab}} \to Z(G)^{\mathrm{ab}} = Z(G)$; by cor.7.8, we have $\mathrm{Ver}(g) = g^n$; since g belongs to $D(G)$, this shows that $g^n = 1$.]
Show that $D(G)$ is finite.
[Hint: show first that $D(G) \cap Z(G)$ is a finitely generated abelian torsion group, hence is finite; conclude that $D(G)$ is finite.]

10. (*Focal subgroup.*) Let S be a p-Sylow subgroup of a finite group G. Let N be the kernel of Ver : $G \to S^{\mathrm{ab}}$. Let $\mathrm{Fo}(S)$ be the subgroup of S generated by all $x^{-1}y$ with $x, y \in S$ and x, y conjugate in G ("focal subgroup" of S).
Show that $\mathrm{Fo}(S) = S \cap D(G) = S \cap N$.
[Hint: the inclusions $\mathrm{Fo}(S) \subset S \cap D(G) \subset S \cap N$ are obvious. To prove that every $g \in S \cap N$ belongs to $\mathrm{Fo}(S)$, use formula (7.3) and deduce that $\prod_\alpha z_\alpha^{-1} g^{f_\alpha} z_\alpha \in D(S)$. Since $z_\alpha^{-1} g^{f_\alpha} z_\alpha = g^{f_\alpha}$ mod $\mathrm{Fo}(S)$, this shows that g^n belongs to the group $\mathrm{Fo}(S)$, where $n = \sum f_\alpha = (G : S)$. Since n is prime to p, this implies $g \in \mathrm{Fo}(S)$.]

11. (*Defining transfer via right cosets instead of left cosets.*) Let H be a subgroup of finite index of a group G. Let Σ be a set of representatives of the right cosets mod H; we have $G = H\Sigma$. Let g be an element of G; for every $\sigma \in \Sigma$, there exists a unique $h_{g,\sigma} \in H$ such that $\sigma g \in h_{g,\sigma}.\Sigma$. Show that $\prod_\sigma h_{g,\sigma} = \mathrm{Ver}(g)$ mod $D(H)$.
[Hint: use the fact that the $(\sigma^{-1})_{\sigma \in \Sigma}$ make up a set of representatives of the left cosets mod H.]

12. (*Relation between the transfer and the Nakayama map.*) Let $1 \to A \to E \to G \to 1$ be an abelian extension of a finite group G ; let $[E]$ be the corresponding element of $H^2(G, A)$, cf. §4.4. Let us write A additively; denote by A^G the subgroup of A fixed under G, and let TA be the subgroup of A^G made up of the $\sum_{g \in G} ga$, for $a \in A$. The transfer homomorphism Ver : $E \to A$ maps E into A^G (prop.7.4), and maps A into TA (cor.7.11), hence defines a homomorphism $v_E : G \to A^G/TA$. Show that v_E is the image of $[E]$ by the Nakayama map $N : H^2(G, A) \to \mathrm{Hom}(G, A^G/TA)$, defined in exerc.5 of chap.4.
[Hint: as in §4.4, let $h : G \to E$ be a section of $E \to G$ and let f be the corresponding 2-cocycle. Show, using exerc.11, that $\mathrm{Ver}(h(y)) = \sum_x f(x, y)$ for every $y \in G$.]

13. (*A Bieberbach group of rank* 2.) Let $C = \{1, c\}$ be a group of order 2, and let $G = H.C$ be the semidirect product of C by the group $H = \mathbf{Z} \times \mathbf{Z}$, the element c acting on H by $(x, y) \mapsto (y, x)$. Let H_0 be the subgroup of H made up of the (x, y) with $x \equiv y \pmod 2$, and let $H_1 = H - H_0$. Show that $\Gamma = H_0 \cup cH_1$ is a nonabelian torsion-free subgroup of index 2 of G, which contains a subgroup of index 2 isomorphic to $\mathbf{Z}^2$.

[The group Γ acts in a natural way on the euclidean space $\mathbf{R}^2$; this action is free, and the quotient space $\mathbf{R}^2/\Gamma$ is a compact non-orientable surface, known as the *Klein bottle*, cf. [40], §2.5.]

14. Give a transfer-free proof of prop.7.12 by applying exerc.7 of chap.4.

15. (*Groups with cyclic Sylow subgroups.*) Let G be a finite group.
a) Assume $G \neq 1$ and let S be a p-Sylow subgroup of G, where p is the smallest prime dividing $|G|$. Assume that S is cyclic. Show that S is contained in the center of $N_G(S)$. [Hint: use the fact that $|\mathrm{Aut}(S)|$ and $|N_G(S)/S|$ are relatively prime.]
Show that $\mathrm{Ver} : G \to S$ is surjective [use th.7.15]; let C be its kernel. Show that C is independent of the choice of S and that $G = CS$.
b) Assume that, for every prime q, the q-Sylow subgroups of G are cyclic. Show that G is supersolvable (cf. chap.3, exerc.13).
[Hint: use induction on $|G|$. If S and C are as in a), then C is supersolvable. If $C \neq 1$, let q be the largest prime dividing $|C|$; by chap.3, exerc.13 e), C has a unique q-Sylow subgroup S', which is normal in G; apply the induction hypothesis to G/S' and use the fact that an extension of a supersolvable group by a cyclic group is supersolvable.]

16. (*Characterization of the integers n such that every group of order n is cyclic.*)
Let n be an integer $\geqslant 1$ and let $\varphi(n) = |(\mathbf{Z}/n\mathbf{Z})^\times|$. Show the equivalence of the following properties:
a) n and $\varphi(n)$ are relatively prime.
b) $n = p_1 \cdots p_m$ where the p_i are distinct primes such that $p_i \not\equiv 1 \pmod{p_j}$ for every i, j.
c) Every group of order n is cyclic.
[Hint for b) $\Longrightarrow$ c): let G be a group of order n, where n has property b). Use exerc.15 to show that G is supersolvable, hence has a normal subgroup of prime order. Show that this subgroup is contained in the center of G, and use induction on m.]

17. (*Characterization of* $\mathrm{PSL}_2(\mathbf{F}_p)$ *when* $p \equiv 3 \pmod 4$.)
Let G be a simple group of order $p(p^2-1)/2$, where p is a prime number $\equiv 3 \pmod 4$. Prove that $G \simeq \mathrm{PSL}_2(\mathbf{F}_p)$.
[Hint: use the same method as for the case $p = 7$, cf. th.7.23 :
a) Let U be a p-Sylow subgroup of G, and let B be its normalizer. Let $d = (G : B)$, and write $|B| = pm$, with $dm = (p^2-1)/2$. Note that $d \equiv 1 \pmod p$, and $d > 1$. Show that $2m + 1 \equiv 0 \pmod p$ and $2m + 1 \leqslant p$, hence $2m + 1 = p$ and $d = p + 1$.
b) Let $X = G/B$; we have $|X| = d = p + 1$. Let ∞ be the point of X fixed under B; the group U acts freely and transitively on $X - \{\infty\}$. Identify X with the projective line $\mathbf{P} = \mathbf{P}_1(\mathbf{F}_p)$ in such a way that U acts by translation on $\mathbf{P} - \{\infty\}$. Show that the centralizer of U is equal to U. Hence the action of B/U on $\mathbf{P} - \{\infty\}$ is faithful.
c) Write B as a semidirect product $B = UT$. Show that T can be chosen such that it fixes the point 0 of $\mathbf{P}$. This implies that the action of T on $\mathbf{P}$ is given by $i \mapsto \lambda i$, with $\lambda \in (\mathbf{F}_p^\times)^2$ (note that T is cyclic of order $m = (p-1)/2$).
d) Let t be a generator of T. Since $G^{\mathrm{ab}} = 1$, the image of t by $\mathrm{Ver} : G^{\mathrm{ab}} \to B^{\mathrm{ab}} \simeq T$ is 1. Use th.7.5 to prove that $\mathrm{Ver}(t) = t.wtw^{-1}$ for some $w \in N_G(T)$, hence $wtw^{-1} = t^{-1}$. Show that w can be chosen of order 2 (use the fact that $|T|$ is odd, since $p \equiv 3 \pmod 4$); determine the action of w on the four orbits of T on $\mathbf{P}$ and deduce that this action is $i \mapsto \lambda/i$ where $-\lambda$ is a square in $\mathbf{F}_p^\times$; hence w belongs to $\mathrm{PSL}_2(\mathbf{F}_p)$. Conclude the proof by showing that B and w generate G, hence G (viewed as a subgroup of $\mathrm{Aut}(\mathbf{P})$) is contained in $\mathrm{PSL}_2(\mathbf{F}_p)$, hence is equal to that group, since it has the same order.]

Chapter 8

Characters

In this chapter, k is a field and G is a group. From section 8.2 on, G is finite and $k = \mathbf{C}$.

8.1 Linear representations and characters

8.1.1. Definitions.

Let V be a finite-dimensional vector space over k.

Definition 8.1. *A **linear representation** of G on V is a group homomorphism*

$$\rho : G \to \mathbf{GL}(V).$$

*The dimension of V is called the **degree** of the representation.*

Remarks. (1) This gives an action of G on V, namely $gx = \rho(g)(x)$ for $x \in V$ and $g \in G$.

(2) One also says that V is a **representation space** of G or simply a **representation** of G. We often write ρ_V instead of ρ.

8.1.2. The group algebra point of view.

Let us recall what the **group algebra** $k[G]$ is (here k does not need to a field - any commutative ring would do) : it is a k-algebra with a basis $(e_g)_{g\in G}$ such that $e_g e_{g'} = e_{gg'}$ if $g, g' \in G$. In practice, e_g is identified with g, and the elements of $k[G]$ are written as

$$\sum_{g\in G} f(g)g,$$

with $f(g) \in k$ and $f(g) = 0$ for every g but a finite number (i.e., f has *finite support*).

If V is a representation of G, the action of G extends by linearity to an action of $k[G]$, so that V becomes a left $k[G]$-module. Conversely, every left $k[G]$-module which is of finite dimension over k defines a linear representation of G. This will allow us to use at will, either the G-representation language, or the $k[G]$-module one.

8.1.3. Examples of representations.

If V and V' are representations of G, so are all the finite-dimensional vector spaces constructed canonically from V and V'. For instance:

(1) The direct sum $V \oplus V'$: $g(x \oplus y) = gx \oplus gy$, for $g \in G$, $x \in V$ and $y \in V'$.

(2) The tensor product $V \otimes V'$: $g(x \otimes y) = gx \otimes gy$.

(3) The dual V^* of V: $(gy)(x) = y(g^{-1}x)$ for $x \in V$, $y \in V^*$.
[Equivalently : $\langle gx, gy \rangle = \langle x, y \rangle$, i.e., the scalar product between V and V^* is G-invariant.]

(4) $\mathrm{Hom}(V, V') \simeq V^* \otimes V'$: $(gh)(x) = gh(g^{-1}x)$ for $h \in \mathrm{Hom}(V, V')$ and $x \in V$.

Other examples: the *exterior powers* $\wedge^n V$ and the *symmetric powers* $\mathrm{Sym}^n V$, $n \geqslant 0$, of a representation V.

8.1.4. Character of a representation.

Let $\rho_V : G \to \mathrm{GL}(V)$ be a linear representation of G of degree n. If $g \in G$, let

$$\chi_V(g) = \mathrm{Tr}\big(\rho_V(g)\big)$$

be the *trace* of $\rho_V(g)$. If $\lambda_1, \dots, \lambda_n$ are the eigenvalues of $\rho_V(g)$ in a suitable extension of k, then :

$$\chi_V(g) = \sum \lambda_i.$$

The function $\chi_V : G \to k$ is called the **character** of the representation V.

Proposition 8.1. (1) χ_V *is a class function*[1].

(2) $\chi_{V \oplus V'} = \chi_V + \chi_{V'}$.

(3) $\chi_{V \otimes V'} = \chi_V \chi_{V'}$.

(4) $\chi_{V^*}(g) = \chi_V(g^{-1})$ *for all* $g \in G$.

(5) $\chi_{\mathrm{Hom}(V,V')}(g) = \chi_V(g^{-1})\chi_{V'}(g)$ *for all* $g \in G$.

(6) $\chi_V(1) = \dim V$.

Assume that k does not have characteristic 2. *Then* :

(7) $\chi_{\wedge^2 V}(g) = \frac{1}{2}(\chi_V(g)^2 - \chi_V(g^2))$.

(8) $\chi_{\mathrm{Sym}^2 V}(g) = \frac{1}{2}(\chi_V(g)^2 + \chi_V(g^2))$.

[1]A function f on a group G is called a **class function** if it is constant on every conjugacy class, or, equivalently, if $f(xy) = f(yx)$ for every $x, y \in G$.

Proof. Formulas (1) to (4) follow from standard properties of traces; formula (5) follows from (3) and from $\mathrm{Hom}(V_1, V_2) \simeq V_1^* \otimes V_2$; formula (6) is obvious. As for (7) and (8), note that, if the eigenvalues of $\rho_V(g)$ are $\lambda_1, \ldots, \lambda_n$, those of $\rho_V(g^2)$ are $\lambda_1^2, \ldots, \lambda_n^2$, and those of $\rho_{\wedge^2 V}(g)$ are the $\lambda_i \lambda_j$ with $i < j$. Equation (7) then follows from the identity

$$(\sum \lambda_i)^2 = \sum \lambda_i^2 + 2 \sum_{i<j} \lambda_i \lambda_j.$$

Equation (8) follows from (7) and the isomorphism $V \otimes V \simeq \wedge^2 V \oplus \mathrm{Sym}^2 V$.

More generally, if $k \geqslant 1$, the character $\lambda^k \chi_V$ of $\wedge^k V$ is the following : its value at $g \in G$ is equal to the coefficient of t^k in the polynomial $\det(1 + t\rho_V(g))$. See also §8.8.2 and exerc.20.

8.1.5. Example : permutation characters.

Let X be a finite G-set, and let $V_X = k^X$ be the product of X copies of k. The vector space V_X has a canonical basis v_x, $x \in X$. We make G act on V_X by its action on X, i.e., $gv_x = v_{gx}$; the representation so obtained is called a *permutation representation.* Its degree is equal to $|X|$. As for its character, we have already met it in chapter 1:

Proposition 8.2. *The character of the permutation representation V_X is the function χ_X of prop.1.1, namely the function* :

$$\chi_X(g) = |X^g| = \text{ number of elements of } X \text{ fixed by } g.$$

[When k has characteristic $p > 0$, the formula should be interpreted mod p, i.e., $\chi_X(g)$ is the residue class of $|X^g|$ mod p.]

Proof. The coefficient of v_x in gv_x is 1 if $gx = x$ and 0 if $gx \neq x$. Hence the trace of the matrix representing g is the number of such 1's, i.e., $\chi_X(g)$.

Assume that G is finite. When one chooses $X = G$, with the action given by left multiplication, the corresponding representation is called the **regular representation** of G. From the $k[G]$-module point of view, it corresponds to $k[G]$, viewed as a module over itself via left multiplications. We shall denote the corresponding character by r_G. Proposition 8.2 gives:

Corollary 8.3. $r_G(g) = \begin{cases} |G| & \text{if } g = 1 \\ 0 & \text{if } g \neq 1. \end{cases}$

8.2 Characters, hermitian forms and irreducible representations

Recall that, from now on, $k = \mathbf{C}$ and the group G is finite.

8.2.1. Basic properties of characters.

Let $\rho : G \to \mathrm{GL}(V)$ be a linear representation of G, let χ_V be its character, and let g be an element of G. The eigenvalues of $\rho(g)$ are *roots of unity*, and hence are complex numbers of absolute value 1. Moreover :

Proposition 8.4. *The endomorphism $\rho(g)$ of V is diagonalizable* (i.e., there exists a basis of V made up of eigenvectors of $\rho(g)$).

Proof. If m is the order of g, the minimal polynomial of $\rho(g)$ divides $t^m - 1$; hence its roots are distinct, which implies (cf. e.g. Bourbaki [4], VII.7, prop.12) that $\rho(g)$ is diagonalizable.
[Alternative proof: use prop.8.9, and the fact that a unitary matrix is diagonalizable, cf. prop.9.10.]

Proposition 8.5. *For every $g \in G$ we have :*

(1) $\chi_V(g^{-1}) = \overline{\chi_V(g)}$.

(2) $|\chi_V(g)| \leqslant \dim V$.

(3) $|\chi_V(g)| = \dim V$ *if only if g acts on V by scalar multiplication.*

(4) $\chi_V(g) = \dim V$ *if and only if g acts trivially on V.*

Proof. Let $n = \dim V$, and let $\lambda_1, \ldots, \lambda_n$ be the eigenvalues of $\rho(g)$. Since $|\lambda_i| = 1$ for every i,, we have $|\lambda_1 + \cdots + \lambda_n| \leqslant n$, which proves (2).
The eigenvalues of $\rho(g^{-1})$ are the $\lambda_j^{-1} = \overline{\lambda_j}$; their sum is $\overline{\chi_V(g)}$, which proves (1).
To prove (3), we use:

Lemma 8.6. *Let $z_1, \ldots, z_n$ be complex numbers of absolute value* 1. *If $|z_1+\cdots+z_n| = n$, then $z_1 = z_2 = \cdots = z_n$.*

Proof of the lemma. Let $z = z_1 + \cdots + z_n$. Write $z_j = e^{i\varphi_j}$ with $\varphi_j \in \mathbf{R}/2\pi\mathbf{Z}$. We have

$$z\overline{z} = \sum_{j,j'} e^{i(\varphi_j - \varphi_{j'})} = n + 2\sum_{j<j'} \cos(\varphi_j - \varphi_{j'}).$$

If the φ_j are not all equal, one of the terms $\cos(\varphi_j - \varphi_{j'})$ is < 1, hence $z\overline{z} < n + n(n-1)$, which contradicts the assumption $|z| = n$. Hence the φ_j are equal, i.e., $z_1 = \cdots = z_n$.

End of the proof of (3) *and* (4). If $|\chi_V(g)| = \dim V$, we have $\lambda_1 + \cdots + \lambda_n = n$; by lemma 8.6, this implies that the λ_i are equal; by prop.8.4, this shows that $\rho(g)$ is a homothety. As for (4), it follows from (3).

Corollary 8.7. *We have $\chi_{V^*} = \overline{\chi_V}$.*

Proof. This follows from part (1) of prop.8.5 and part (4) of prop.8.1.

8.2.2. Invariant hermitian forms.

Let V be a finite-dimensional **C**-vector space. Recall that a *hermitian form* on V is an **R**-bilinear map $h : V \times V \to \mathbf{C}$ such that

$$h(y,x) = \overline{h(x,y)} \text{ and } \lambda h(x,y) = h(\lambda x, y) = h(x, \overline{\lambda} y) \text{ for } x, y \in V, \ \lambda \in \mathbf{C}.$$

[Note that we are asking linearity in the first variable and antilinearity in the second variable. The opposite convention is equally frequent, especially in Physics. Compare, e.g., Lang [29], XIII, §7 and Fulton-Harris [20], §2.2.]

This implies $h(x,x) \in \mathbf{R}$ for every $x \in V$. The **R**-quadratic form $q_h : x \mapsto h(x,x)$ determines h uniquely, via the formula:

$$4h(x,y) = \sum_{\omega^4=1} \omega q_h(x + \omega y) = q_h(x+y) - q_h(x-y) + iq_h(x+iy) - iq_h(x-iy).$$

The form h is said to be *positive definite* if $h(x,x) > 0$ for every $x \in V$, $x \neq 0$.

Example. If $V = \mathbf{C}^n$, the hermitian form $h_n(x,y) = \sum x_i \overline{y_i}$ is positive definite; every positive definite hermitian form on $\mathbf{C}^n$ can be transformed into h_n by a suitable change of coordinates.

Proposition 8.8. *Let h be a positive definite hermitian form on V. Let W be a subspace of V and let W' be its orthogonal for h* (i.e., the set of $x \in V$ such that $h(x,y) = 0$ for every $y \in W$). *Then W' is a subspace of V and $V = W \oplus W'$.*

Proof. Let $(e_1, \dots, e_m)$ be a basis of W; the set W' is defined by the vanishing of the m linear forms $x \mapsto h(x, e_i)$; hence it is a subvectorspace of dimension $m' \geqslant n - m$, where $n = \dim V$. If $x \in W \cap W'$, we have $h(x,x) = 0$, hence $x = 0$. This shows that $W \cap W' = 0$, hence $m + m' \leqslant n$, hence $m + m' = n$ and $V = W \oplus W'$.

Proposition 8.9. *Let V be a linear representation of G. There exists a positive definite hermitian form on V that is invariant by G.*

Proof. Choose a positive definite hermitian form h_0 on V, for instance the form h_n above, relative to a **C**-isomorphism $V \simeq \mathbf{C}^n$. Define

$$h(x,y) = \sum_{g \in G} h_0(gx, gy).$$

It is hermitian, positive definite, and invariant by G.

[Proposition 8.9 is equivalent to saying that every finite subgroup of $\mathrm{GL}_n(\mathbf{C})$ is conjugate to a subgroup of the unitary group $\mathbf{U}_n(\mathbf{C})$. This is a special case of a general result on compact subgroups of $\mathrm{GL}_n(\mathbf{C})$, which is proved in the same way, the summation over G being replaced by integration with respect to a Haar measure.]

8.2.3. Splitting of linear representations.

Proposition 8.10. *Let W be a G-invariant subspace of V.*
(1) *There exists a G-invariant subspace of V complementary to W.*
(2) *Every G-invariant element of V/W is the image of a G-invariant element of V.*

Proof. Choose a G-invariant positive definite hermitian form h on V. Let W' be the orthogonal of W for h. By prop.8.8, we have $V = W \oplus W'$, and it is clear that W' is G-invariant. This proves (1); as for (2), it follows from (1).

Alternative proof for (2):

If $z \in V/W$ is G-invariant, choose a representative x of z in V, and define $\tilde{z} \in V$ by $\tilde{z} = \frac{1}{|G|} \sum_{g \in G} gx$. The element $\tilde{z}$ is G-invariant and its image in V/W is z.

Alternative proof for (1):

Apply (2) to the surjective homomorphism $\mathrm{Hom}(V, W) \to \mathrm{Hom}(W, W)$, and to the G-invariant element $z = \mathrm{id}_W$ of $\mathrm{Hom}(W, W)$. We obtain an element f of $\mathrm{Hom}(V, W)$ that is G-invariant, i.e., commutes with the action of G, and whose restriction to W is id_W. Then $\mathrm{Ker} f$ is G-invariant, and $V = W \oplus \mathrm{Ker} f$.

[Note that these alternative proofs do not require k to be $\mathbf{C}$. They work over any field in which $|G|$ is invertible.]

8.2.4. Irreducible representations.

Definition 8.2. *Let $\rho : G \to \mathbf{GL}(V)$ be a linear representation of G. It is* ***irreducible*** *if $V \neq 0$ and there is no G-invariant subspace of V distinct from 0 and V.*

Remark. We may view V as a *group with operators* in the sense of the Remark at the end of §1.3, the set Φ of operators being the disjoint union of G and $\mathbf{C}$ (acting by scalar multiplication). The above definition simply means that V is simple as a Φ-group. From the module point of view of §8.1.2, it means that V is a simple left $k[G]$-module.

Theorem 8.11. *Every representation is a direct sum of irreducible representations.*

Proof. Use induction on $\dim V$. There is nothing to prove if $\dim V \leqslant 1$. If $\dim V > 1$, either V is irreducible (and we are done), or there exists a proper G-invariant subspace $V' \neq 0$ of V. Then, by prop.8.10, there exists a direct sum decomposition of $V = V' \oplus V''$ with $\dim V' < \dim V$ and $\dim V'' < \dim V$, where V' and V'' are G-invariant. Applying the induction hypothesis to V' and V'', we obtain a direct sum decomposition for V.

8.3 Schur's lemma

Theorem 8.12 (Schur's lemma[2], [34], n°7). *Let $\rho_1 : G \to \mathbf{GL}(V_1)$ and $\rho_2 : G \to \mathbf{GL}(V_2)$ be two irreducible representations of G. Let $f : V_1 \to V_2$ be a G-morphism, i.e., a linear map such that $\rho_2(g) \circ f = f \circ \rho_1(g)$ for all $g \in G$. Then :*

(1) *If V_1 and V_2 are not isomorphic, then $f = 0$.*

(2) *If $V_1 = V_2$ and $\rho_1 = \rho_2$, then f is a homothety.*

Proof. (1) If $x \in \operatorname{Ker} f$, we have $f(\rho_1(g))(x) = \rho_2(g)(f(x)) = 0$ for all $g \in G$. Thus, $\operatorname{Ker} f$ is G-invariant. Since V_1 is irreducible, either $\operatorname{Ker} f = 0$ or $\operatorname{Ker} f = V_1$. In the first case, f is injective, and in the second case $f = 0$. Similarly, $\operatorname{Im} f$ is G-invariant, hence either $\operatorname{Im} f = 0$ or $\operatorname{Im} f = V_2$. Thus, if $f \neq 0$, we have $\operatorname{Ker} f = 0$ and $\operatorname{Im} f = V_2$, hence f is an isomorphism from V_1 to V_2. This proves (1).

(2) Let $V_1 = V_2$ and $\rho = \rho_1 = \rho_2$. Let $\lambda \in \mathbf{C}$ be an eigenvalue of f. Let $f' = f - \lambda$. Then f' is not injective. On the other hand, $\rho(g) \circ f' = \rho(g) \circ (f - \lambda) = f' \circ \rho(g)$. Thus, by (1), we have $f' = 0$, hence f is a homothety.

Corollary 8.13. $\dim \operatorname{Hom}_G(V_1, V_2) = 1$ *if* $V_1 \simeq V_2$, *and* $\operatorname{Hom}_G(V_1, V_2) = 0$ *otherwise.*

[Here, $\operatorname{Hom}_G(V_1, V_2)$ denotes the space of all the G-homomorphisms of V_1 into V_2.]

Corollary 8.14. *If G is abelian, its irreducible representations are* 1*-dimensional* (i.e., they are given by homomorphisms $G \to \mathrm{GL}_1(\mathbf{C}) = \mathbf{C}^\times$).

Proof. Let V be an irreducible representation of G. By part (2) of Schur's lemma, the elements of G act by homotheties; this implies that $\dim V = 1$.

Remark. Both Schur's lemma and cor.8.14 are valid (with the same proofs) for arbitrary groups and for arbitrary algebraically closed fields.

8.4 Orthogonality relations

Let f_1 and f_2 be functions on G. Their **scalar product** $\langle f_1, f_2 \rangle$ is defined by:

$$\langle f_1, f_2 \rangle = \frac{1}{|G|} \sum_{g \in G} f_1(g) f_2(g^{-1}). \tag{8.1}$$

It is symmetrical : $\langle f_1, f_2 \rangle = \langle f_2, f_1 \rangle$.

Remark. If χ is a character, then $\chi(g^{-1}) = \overline{\chi(g)}$, cf. prop.8.5. Hence $\langle f, \chi \rangle$ can also be viewed as a hermitian scalar product:

$$\langle f, \chi \rangle = \frac{1}{|G|} \sum_{g \in G} f(g) \overline{\chi(g)}. \tag{8.2}$$

[2]In his paper, Schur mentions that this lemma had already been used by Burnside.

Theorem 8.15 (Basic formula). *Let V be a linear representation of G, and let V^G be the subspace of V fixed by G. Then :*

$$\dim V^G = \langle \chi_V, 1 \rangle = \frac{1}{|G|} \sum_{g \in G} \chi_V(g). \tag{8.3}$$

[In $\langle \chi_V, 1 \rangle$, the symbol " 1 " means the constant function on G equal to 1.]

Proof. Let π be the endomorphism $x \mapsto \frac{1}{|G|} \sum_{g \in G} gx$ of V. We have $\pi x \in V^G$ for every x, and $\pi x = x$ if $x \in V^G$; this implies that $\pi^2 = \pi$, i.e., that π is an idempotent; its image is V^G. We thus get a splitting : $V = \text{Im } \pi \oplus \text{Ker } \pi$. In that splitting, π is the identity on the first factor and is 0 on the second factor. Its trace is thus the dimension of the first factor, i.e., $\dim V^G$. Since $\text{Tr}(\pi) = \frac{1}{|G|} \sum_{g \in G} \text{Tr } \rho_V(g) = \frac{1}{|G|} \sum_{g \in G} \chi_V(g)$, we obtain formula (8.3).

Example. Let X be a finite G-set, and let $V = V_X$ be the corresponding permutation representation, cf. §8.1.5. An element v of V may be viewed as a function $v : X \to \mathbf{C}$. It is G-invariant if and only if it is constant on every orbit of G. This shows that $\dim V^G = |X/G|$. Hence $|X/G| = \langle 1, \chi_X \rangle$: we recover prop.1.1 (Burnside's lemma).

Proposition 8.16. *Let χ and χ' be the characters of two representations V and V' of G. Then :*

$$\langle \chi, \chi' \rangle = \dim \text{Hom}_G(V', V). \tag{8.4}$$

[Recall that $\text{Hom}_G(V', V)$ denotes the space of all the G-homomorphisms of V' into V.]

Proof. View $W = \text{Hom}(V', V)$ as a representation of G. Its character is equal to $\chi\overline{\chi'}$, cf. prop.8.1. An element f of W is fixed under G if and only if it is a G-homomorphism of V' into V. By th.8.4, we have $\dim W^G = \langle \chi\overline{\chi'}, 1 \rangle = \langle \chi, \chi' \rangle$.

Corollary 8.17 (Orthogonality of irreducible characters). *Suppose that V and V' are irreducible. Then :*

$$\langle \chi, \chi' \rangle = \begin{cases} 1 & \textit{if } V \textit{ is isomorphic to } V', \\ 0 & \textit{otherwise.} \end{cases}$$

Proof. This follows from prop.8.16 and cor.8.13.

The characters of the irreducible representations of G are called the **irreducible characters** of G.

Corollary 8.18. *The irreducible characters of G are $\mathbf{C}$-linearly independent.*

Proof. This follows from the orthogonality property of cor.8.17.

Remark. The last corollary is also true when G is infinite; it is a consequence of a general result on representations of algebras, applied to the group algebra $\mathbf{C}[G]$ of G, see e.g. Bourbaki [5], §20.6, prop.6.

Theorem 8.19. *Let V be a representation with character χ_V and let $V = \bigoplus_\alpha V_\alpha$ be a splitting of V into a direct sum of irreducible representations V_α. Let W be an irreducible representation of G. The number of V_α's that are isomorphic to W does not depend on the chosen splitting ; it is equal to $\langle \chi_V, \chi_W \rangle$.*

Proof. We have $\chi_V = \sum_\alpha \chi_{V_\alpha}$, hence $\langle \chi_V, \chi_W \rangle = \sum_\alpha \langle \chi_{V_\alpha}, \chi_W \rangle$. By cor.8.17, $\langle \chi_{V_\alpha}, \chi_W \rangle$ is 1 or 0 depending on whether V_α is isomorphic to W or not.

Remark. The part about the independence on the chosen splitting is also a consequence of Jordan-Hölder's theorem for $k[G]$-modules, cf. §8.1.2; no assumptions on G, nor on the ground field, are necessary.

Corollary 8.20. *Two representations with the same character are isomorphic.*

[The characters deserve their name: they *characterize* the representations.]

Proof. Indeed, if we split the two representations in direct sums of irreducible ones, th.8.19 shows that each irreducible representation W occurs the same number of times.

Remark. This corollary remains true for the linear representations of any group, over a field k, provided that the characteristic of k is 0 and that the two representations are semisimple, i.e., direct sums of irreducible representations, cf. Bourbaki, [5], §20.6, cor. to prop.6.

Let us now apply the above to the regular representation, and its character r_G, cf. §8.1.5:

Proposition 8.21. *Let* $\mathrm{Irr}(G)$ *be the set of irreducible characters of* G. *Then :*

(1) $r_G = \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)\chi$.

(2) $|G| = \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)^2$.

(3) $\sum_{\chi \in \mathrm{Irr}(G)} \chi(1)\chi(g) = 0$ *for every* $g \in G,\ g \neq 1$.

[Note that $\mathrm{Irr}(G)$ is finite: this follows from cor.8.18.]

Proof. The values of $r_G(g)$ given in cor.8.3 show that $\langle \chi, r_G \rangle = \chi(1)$; this proves formula (1). Formulas (2) and (3) follow.

8.5 Structure of the group algebra and of its center

Let $\mathrm{Irr}(G)$ be the set of irreducible characters of G; for each $\chi \in \mathrm{Irr}(G)$, let W_χ be a representation of G with character χ; recall that $\chi(1) = \dim W_\chi$.

8.5.1. Structure of the group algebra $\mathbf{C}[G]$.

Since W_χ is a $\mathbf{C}[G]$-module, we have a natural homomorphism $r_\chi : \mathbf{C}[G] \to \mathrm{End}(W_\chi)$. Its restriction to G is $\rho_\chi : G \to \mathrm{GL}(W_\chi)$.

The family (r_χ) define an algebra homomorphism:

$$r = (r_\chi) : \mathbf{C}[G] \to \prod_{\chi \in \mathrm{Irr}(G)} \mathrm{End}(W_\chi). \tag{8.5}$$

Theorem 8.22. *The map $r : \mathbf{C}[G] \to \prod_{\chi \in \mathrm{Irr}(G)} \mathrm{End}(W_\chi)$ is an isomorphism.*

Proof. By part (2) of prop.8.21, we have $|G| = \sum \chi(1)^2$; this shows that the two algebras have the same dimension. Hence we only have to prove that r is injective, which is clear: an element of $\mathrm{Ker}(r)$ acts by 0 on every linear representation of G, in particular on the regular representation, hence is 0.

Here is an explicit formula for the inverse of r :

Theorem 8.23. *Let (u_χ) be an element of $\prod_{\chi \in \mathrm{Irr}} \mathrm{End}(W_\chi)$. If $g \in G$, put*

$$\lambda_g = \frac{1}{|G|} \sum_{\chi \in \mathrm{Irr}(G)} \chi(1) \mathrm{Tr}(g^{-1} u_\chi). \tag{8.6}$$

Then $r(\sum_{g \in G} \lambda_g g) = (u_\chi)$.

[In formula (8.6), $\mathrm{Tr}(g^{-1}u_\chi)$ means the trace of the endomorphism $\rho_\chi(g^{-1})u_\chi$ of W_χ.]

Proof. Let us consider first the case where $u_\chi = \rho_\chi(x)$, where x is a given element of G. In that case, we have

$$\lambda_g = \frac{1}{|G|} \sum_\chi \chi(1)\chi(g^{-1}x) = \frac{1}{|G|} r_G(g^{-1}x),$$

which is 0 if $x \neq g$ and 1 if $x = g$, cf. prop.8.21. Hence $\sum_{g \in G} \lambda_g g = x$, and we indeed have $r(x) = (\rho_\chi(x))$. The general case follows by additivity, since the vector space $\prod_{\chi \in \mathrm{Irr}(G)} \mathrm{End}(W_\chi)$ is spanned by the image of G.

8.5.2. Structure of the center of $\mathbf{C}[G]$.

If R is a ring, its **center** R^{cent} is defined in the same way as for groups, i.e., as the set of $x \in R$ such that $xy = yx$ for every $y \in R$; it is a commutative subring of R.

The center $\mathbf{C}[G]^{\mathrm{cent}}$ of $\mathbf{C}[G]$ is made up of the $\sum f(g)g$ where f is a class function on G; its dimension is the number h of conjugacy classes of G.

Theorem 8.24. *The isomorphism $r : \mathbf{C}[G] \to \prod_\chi \mathrm{End}(W_\chi)$ of th.8.22 induces an isomorphism $\omega : \mathbf{C}[G]^{\mathrm{cent}} \to \mathbf{C}^{\mathrm{Irr}(G)} = \mathbf{C} \times \cdots \times \mathbf{C}$ (copies indexed by $\chi \in \mathrm{Irr}(G)$).*

Proof. This follows from th.8.22, and the fact that the center of $\mathrm{End}(W_\chi)$ is $\mathbf{C}$.

Corollary 8.25. *$|\mathrm{Irr}(G)| = h$, i.e., the number of irreducible characters of G is equal to the number of conjugacy classes of G.*

Proof. This follows from $\dim \mathbf{C}[G]^{\text{cent}} = h$ and $\dim \mathbf{C}^{\text{Irr}(G)} = |\text{Irr}(G)|$.

Equivalently:

Corollary 8.26. *The irreducible characters make up a basis of the space of class functions.*

Corollary 8.27. *Two elements g and g' of G are conjugate if and only if $\chi(g') = \chi(g)$ for every character χ of G.*

Let us now give formulas for computing the isomorphism $\omega : \mathbf{C}[G]^{\text{cent}} \to \mathbf{C}^{\text{Irr}(G)}$ and its inverse.

We start with the χ-component of ω, which is a homomorphism $\omega_\chi : \mathbf{C}[G]^{\text{cent}} \to \mathbf{C}$.

Proposition 8.28. *For every element $\sum_{g\in G} f(g)g$ of $\mathbf{C}[G]^{\text{cent}}$, we have :*

$$\omega_\chi\Big(\sum_{g\in G} f(g)g\Big) = \frac{1}{\chi(1)}\sum_{g\in G} f(g)\chi(g) = \frac{|G|}{\chi(1)}\langle f, \overline{\chi}\rangle. \tag{8.7}$$

Proof. By definition, $\omega_\chi(\sum_g f(g)g)$ is the scalar factor of the homothety of W_χ given by $\sum_g f(g)g$; hence it is equal to the trace of that homothety divided by $\chi(1)$; since that trace is equal to $\sum_g f(g)\chi(g)$, we obtain (8.7).

Here is a formula for $\mathbf{C}^{\text{Irr}(G)} \to \mathbf{C}[G]^{\text{cent}}$:

If $\chi \in \text{Irr}(G)$, let e_χ be the element of $\mathbf{C}^{\text{Irr}(G)}$ whose χ-component is 1, while the other ones are 0. The $(e_\chi)_{\chi\in\text{Irr}(G)}$ make up a basis of $\mathbf{C}^{\text{Irr}(G)}$. They are *orthogonal idempotents*, i.e., we have $e_\chi^2 = e_\chi$ and $e_\chi.e_\psi = 0$ if $\chi \neq \psi$; moreover $\sum e_\chi = 1$.

Let $\varepsilon_\chi \in \mathbf{C}[G]^{\text{cent}}$ be the image of e_χ by the isomorphism $\mathbf{C}^{\text{Irr}(G)} \to \mathbf{C}[G]^{\text{cent}}$; it is an idempotent of $\mathbf{C}[G]^{\text{cent}}$.

Proposition 8.29. *We have*

$$\varepsilon_\chi = \frac{\chi(1)}{|G|}\sum_{g\in G}\chi(g^{-1})g. \tag{8.8}$$

Proof. The image of ε_χ in $\text{End}(W_\chi)$ is 1, and its image in $\text{End}(W_\psi)$ is 0 if $\psi \neq \chi$. Equation (8.6), applied to $u_\chi = 1$ and $u_\psi = 0$ if $\psi \neq \chi$, gives (8.8).

Remark. The idempotents (ε_χ) give a canonical splitting of every linear representation V of G: if we define $V_\chi \subset V$ as $\varepsilon_\chi V$, we have

$$V = \bigoplus_{\chi\in\text{Irr}(G)} V_\chi\,, \tag{8.9}$$

and each V_χ is a direct sum of copies of W_χ. One can go further : for each χ, define $E(V,\chi) = \text{Hom}_G(W_\chi, V)$; the natural map $E(V,\chi)\otimes W_\chi \to V_\chi$ is an isomorphism, and we then have a canonical isomorphism:

$$V \simeq \bigoplus_{\chi \in \mathrm{Irr}(G)} E(V,\chi) \otimes W_\chi. \tag{8.10}$$

Note that this is an isomorphism of G-spaces, provided we make G act trivially on each $E(V,\chi)$. Moreover, it is *functorial* in the following sense :

if V' is another representation of G, any G-homomorphism $V \to V'$ defines linear maps $E(V,\chi) \to E(V',\chi)$ and we obtain in this way an isomorphism

$$\mathrm{Hom}_G(V,V') \to \prod_{\chi \in \mathrm{Irr}(G)} \mathrm{Hom}_{\mathbf{C}}(E(V,\chi), E(V',\chi)).$$

In category parlance, we have an *equivalence* between the following two categories :
- linear representations of G ;
- families (E_χ) of finite-dimensional $\mathbf{C}$-vector spaces indexed by $\mathrm{Irr}(G)$.

8.6 Integrality properties

We recall a few definitions.

8.6.1. Integral elements.

Let x be an element of a commutative ring R.

Proposition 8.30. *The following properties are equivalent :*

(1) *There exist an integer $n \geqslant 1$, and elements $a_1, \dots, a_n$ of $\mathbf{Z}$ such that :*

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0. \tag{8.11}$$

(2) *The subring $\mathbf{Z}[x]$ of R is a finitely generated $\mathbf{Z}$-module.*
(3) *The ring $\mathbf{Z}[x]$ is contained in a finitely generated $\mathbf{Z}$-submodule of R.*

Proof. Equation (8.11) implies that $\mathbf{Z}[x]$ is additively generated by $1, x, \dots, x^{n-1}$; hence (1) implies (2). Conversely, suppose that (2) holds; for every $i \geqslant 0$, let L_i be the $\mathbf{Z}$-module generated by $1, x, \dots, x^i$; we have $L_0 \subset L_1 \subset \dots$ and the union of the L_i is $\mathbf{Z}[x]$; since $\mathbf{Z}[x]$ is finitely generated, we have $L_m = L_{m+1} = \cdots = \mathbf{Z}[x]$ for m large enough. This implies $x^{m+1} \in L_m$, i.e., that we have an equation of type 8.11 for $n = m+1$. Hence (1) and (2) are equivalent. It is clear that (2) implies (3); the converse is true because every submodule of a finitely generated $\mathbf{Z}$-module is finitely generated, see e.g. Bourbaki [4], chap.VII, §3, cor. to prop.1.

An element x having properties (1), (2) and (3) is called **integral over Z**, or **Z-integral**; when the ring R is contained in a field of characteristic 0, one also says that x is an **algebraic integer**.

Proposition 8.31. *The set of* $\mathbf{Z}$*-integral elements of* R *is a subring of* R.

Proof. Let x, y be $\mathbf{Z}$-integral elements of R. Then the ring $P = \mathbf{Z}[x] \otimes_{\mathbf{Z}} \mathbf{Z}[y]$ is finitely generated over $\mathbf{Z}$. The subring $\mathbf{Z}[x, y]$ of R generated by x and y is isomorphic to a quotient of P, hence is finitely generated. Property (3) shows that every element of that ring is $\mathbf{Z}$-integral. Hence $x + y$ and xy are $\mathbf{Z}$-integral; the proposition follows.

Proposition 8.32. *An element of* $\mathbf{Q}$ *is* $\mathbf{Z}$*-integral if and only if it belongs to* $\mathbf{Z}$.

Proof. If $x \in \mathbf{Q}$ is $\mathbf{Z}$-integral, it satisfies an equation of type (8.11):

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0, \quad \text{with} \quad a_i \in \mathbf{Z}.$$

If we write x as p/q, with (p, q) relatively prime, this equation gives

$$p^n + a_1 p^{n-1} q + \cdots + a_n q^n = 0;$$

it implies that p^n is divisible by q; hence $q = \pm 1$ and $x = \pm p$ belongs to $\mathbf{Z}$.

The *roots of unity* (in any field) are obviously $\mathbf{Z}$-integral. We shall need later the following result:

Lemma 8.33. *Let* $x_1, \ldots, x_n \in \mathbf{C}$ *be roots of unity. Suppose that* $x = (x_1 + \cdots + x_n)/n$ *is an algebraic integer. Then, either* $x = 0$, *or* $x_1 = \cdots = x_n$.

Proof. Choose a finite Galois extension $K/\mathbf{Q}$, contained in $\mathbf{C}$, and containing all the x_i; let $\Gamma = \mathrm{Gal}(K/\mathbf{Q})$. Since x is $\mathbf{Z}$-integral, the same is true of all the $\gamma(x), \gamma \in \Gamma$, and also of their product $X = \prod_{\gamma \in \Gamma} \gamma(x)$. Since X is Γ-invariant, it belongs to $\mathbf{Q}$; prop.8.32 then shows that it belongs to $\mathbf{Z}$. Each $\gamma(x)$ is a sum of n roots of unity, divided by n. We thus have $|\gamma(x)| \leqslant 1$, hence $|X| \leqslant 1$. Since X is an integer, it is equal to 0, or to ± 1. In the first case, one of the $\gamma(x)$ is 0; this implies that all of them are 0, hence $x = 0$. In the second case, all the $|\gamma(x)|$ are equal to 1. We then have $|x| = 1$. By lemma 8.6, this implies $x_1 = \cdots = x_n$.

8.6.2. Integrality properties of characters.

Proposition 8.34. *The values of a character are algebraic integers.*

Proof. Indeed, they are sums of roots of unity.

Theorem 8.35. *Let* f *be a class function on* G *such that* $f(g)$ *is an algebraic integer for every* $g \in G$.
(1) *The element* $x = \sum_g f(g)g$ *of* $\mathbf{C}[G]^{\text{cent}}$ *is* $\mathbf{Z}$*-integral.*
(2) *If* $\chi \in \mathrm{Irr}(G)$, *then* $\frac{1}{\chi(1)} \sum_g f(g)\chi(g)$ *is an algebraic integer.*

Proof of (1). Let $R = \mathbf{C}[G]^{\text{cent}}$, and let $R_{\mathbf{Z}}$ be the subring of R made up of the $\sum_g \varphi(g)g$ where φ is a class function with values in $\mathbf{Z}$. If σ is a conjugacy class of G, the element $x_\sigma = \sum_{g\in\sigma} g$ belongs to $R_{\mathbf{Z}}$; the family (x_σ) is a $\mathbf{Z}$-basis of $R_{\mathbf{Z}}$. This shows that $R_{\mathbf{Z}}$ is a free $\mathbf{Z}$-module of finite rank; hence its elements are $\mathbf{Z}$-integral. By assumption, x is a linear combination $\sum \lambda_\sigma x_\sigma$, where the λ_σ are $\mathbf{Z}$-integral; by prop.8.31 this implies that x is $\mathbf{Z}$-integral.

Proof of (2). The homomorphism $\omega_\chi : \mathbf{C}[G]^{\text{cent}} \to \mathbf{C}$ of prop.8.28 maps x to $\frac{1}{\chi(1)} \sum_g f(g)\chi(g)$. Since x is $\mathbf{Z}$-integral, the same is true for its image in $\mathbf{C}$ by ω_χ.

Corollary 8.36. *If $\chi \in \mathrm{Irr}(G)$, then $\chi(1)$ divides $|G|$.*

Proof. Part (2) of th.8.35, applied to $f = \overline{\chi}$, shows that $|G|/\chi(1)$ is an algebraic integer; by prop.8.32, this means that $\chi(1)$ divides $|G|$.

Proposition 8.37. *Let χ be an irreducible character, and let ρ_χ be a linear representation corresponding to χ. Let $g \in G$ and let $c(g)$ be the number of elements of the conjugacy class of g. Then :*

(1) $c(g)\chi(g)/\chi(1)$ is an algebraic integer.

Assume moreover that $c(g)$ and $\chi(1)$ are relatively prime. Then :

(2) $\chi(g)/\chi(1)$ is an algebraic integer.

(3) If $\chi(g) \neq 0$, then $\rho_\chi(g)$ is a homothety.

Proof of (1). Let f be the class function on G which is equal to 1 on the class of g, and vanishes elsewhere. We have $\sum_{z\in G} f(z)\chi(z) = c(g)\chi(g)$. Part (2) of th.8.35 shows that $c(g)\chi(g)/\chi(1)$ is an algebraic integer.

Proof of (2). Since $c(g)$ and $\chi(1)$ are relatively prime, there exist $a, b \in \mathbf{Z}$ such that $ac(g) + b\chi(1) = 1$. Therefore,

$$\frac{\chi(g)}{\chi(1)} = ac(g)\frac{\chi(g)}{\chi(1)} + b\chi(g).$$

By prop.8.34 and by (1), $\chi(g)$ and $c(g)\chi(g)/\chi(1)$ are algebraic integers; hence the same is true for $\chi(g)/\chi(1)$.

Proof of (3). This follows from (2) and from lemma 8.33 applied to the eigenvalues of $\rho_\chi(g)$.

8.7 Galois properties of characters

We first review a few facts on roots of unity.

8.7.1. Cyclotomic fields.

Let N be an integer $\geqslant 1$, and let μ_N be the subgroup of $\mathbf{C}^\times$ made up of the N-th roots of unity. The subfield $K_N = \mathbf{Q}(\mu_N)$ of $\mathbf{C}$ generated by the elements of μ_N is a Galois extension of $\mathbf{Q}$, known as the N-th **cyclotomic field**. Let Σ_N be its Galois group. If $\sigma \in \Sigma_N$, the action of σ on μ_N is given by $z \mapsto z^{a(\sigma)}$, for a unique $a(\sigma) \in (\mathbf{Z}/N\mathbf{Z})^\times$; this follows from the fact that μ_N is cyclic of order N.

Theorem 8.38 (Irreducibility of the cyclotomic polynomial)**.** *The map $a : \sigma \mapsto a(\sigma)$ is an isomorphism of Σ_N onto $(\mathbf{Z}/N\mathbf{Z})^\times$.*

Proof. The fact that a is injective is clear. Its surjectivity was proved in 1801 by Gauss when N is a prime number, and in 1854 by Kronecker in the general case. Proofs can be found in Lang [31], chap.6, th.3.1 and in Bourbaki [4], chap.V, §11, th.2.

Corollary 8.39. *The field K_N is an abelian extension of $\mathbf{Q}$ of degree $\varphi(N) = |(\mathbf{Z}/N\mathbf{Z})^\times|$.*

If m is an integer which is prime to N, we shall denote by σ_m the corresponding automorphism of K_N; it is characterized by :

$$\sigma_m(z) = z^m \quad \text{for every } z \in \mu_N. \tag{8.12}$$

Examples. If $m = 1$, then σ_m is the identity; if $m = -1$, σ_m is the complex conjugation $z \mapsto \overline{z}$, for $z \in K_N$.

Corollary 8.40. *For every integer m prime to N, there exists an automorphism of $\mathbf{C}$ which coincides with σ_m on K_N.*

Proof. Since $\mathbf{C}$ is algebraically closed, every automorphism of K_N can be extended to an automorphism of $\mathbf{C}$, cf. Bourbaki [4], chap.V, §14, cor.1 to prop.8.

8.7.2. Galois action on characters.

We now choose for N the *exponent* of G, i.e., the smallest integer > 0 such that $g^N = 1$ for every $g \in G$. Denote by A_N the subring of K_N generated by the N-th roots of unity; the elements of A_N are algebraic integers[3]. If χ is a character of G, we have $\chi(g) \in A_N$ for every $g \in G$. If m is an integer prime to N, we may apply the automorphism σ_m of §8.7.1 to the values of χ; this gives a function $\sigma_m(\chi) : G \to A_N$.

Theorem 8.41. (1) *The function $\sigma_m(\chi)$ is a character of G.*

(2) $\chi \in \mathrm{Irr}(G) \Longrightarrow \sigma_m(\chi) \in \mathrm{Irr}(G)$.

(3) $\sigma_m(\chi)(g) = \chi(g^m)$ *for every* $g \in G$.

[3]Conversely, every algebraic integer of K_N belongs to A_N, cf. Lang [31], chap.IV, th.4.

Proof. Let $\rho : G \to \mathrm{GL}_n(\mathbf{C})$ be a linear representation of G with character χ. Let $\sigma \in \mathrm{Aut}(\mathbf{C})$ be an automorphism of $\mathbf{C}$ extending σ_m, cf. cor.8.40, and let σ' be the corresponding automorphism of $\mathrm{GL}_n(\mathbf{C})$. The homomorphism $\sigma' \circ \rho : G \to \mathrm{GL}_n(\mathbf{C})$ is a linear representation of G with character $\sigma \circ \chi = \sigma_m(\chi)$. This proves (1). If ρ is irreducible, the same is true of $\sigma' \circ \rho$, which proves (2). If $g \in G$, and the eigenvalues of $\rho(g)$ are $\lambda_1, \ldots, \lambda_n$, those of $\sigma'(\rho(g))$ are the $\sigma(\lambda_i) = \lambda_i^m$, i.e., the eigenvalues of $\rho(g^m)$; their sum is $\chi(g^m)$, which proves (3).

8.7.3. The field of rationality of an element of G.

If m is an integer prime to N, the map $g \mapsto g^m$ is a permutation of the set G which only depends on the residue class of m mod N; we may then view $\Sigma_N = (\mathbf{Z}/N\mathbf{Z})^\times$ as a subgroup of $\mathcal{S}_G$.

Proposition 8.42. *Let $g \in G$ and let $\Sigma_{N,g}$ be the subgroup of Σ_N made up of the m such that g^m is conjugate to g. Let K_g be the subfield of K_N fixed under the action of $\Sigma_{N,g}$. Then :*
(1) We have $\chi(g) \in K_g$ for every character χ of G.
(2) The field K_g is the smallest field containing all the $\chi(g)$.

Proof. Let K'_g be the subfield of K_N generated by all the $\chi(g)$. An element σ_m of Σ_N fixes K'_g if and only if if fixes all the $\chi(g)$; by part (3) of th.8.41, this means that $\chi(g) = \chi(g^m)$ for every χ, i.e., that g and g^m are conjugate (cor.8.27), i.e., if and only if $\sigma_m \in \Sigma_{N,g}$. By Galois theory, this implies $K'_g = K_g$; hence (1) and (2).

The field K_g is called the *field of rationality* of g (or of the conjugacy class of g).

Examples.

(1) When $K_g = \mathbf{Q}$, the element g is said to be *rational*; we then have $\chi(g) \in \mathbf{Z}$ for every character χ. This occurs if and only if $\Sigma_{N,g} = \Sigma_N$, i.e., if and only if g is conjugate to every g^m with m prime to N. If $C_g = \langle g \rangle$ is the cyclic group generated by g, this is equivalent to saying that all the generators of C_g are G-conjugate.
If G is a symmetric group $\mathcal{S}_n$, all the elements of G are rational.

(2) When $K_g \subset \mathbf{R}$, the element g is said to be *real*. This happens if and only if g and g^{-1} are G-conjugate.

(3) Let $G = \mathrm{PSL}_2(\mathbf{F}_p)$, where p is a prime number $\neq 2$, and choose g of order p. Let $C_p = \langle g \rangle$ be the subgroup generated by g, and let $B = N_G(C_p)$; the image of B in $\mathrm{Aut}(C_g) \simeq \mathbf{F}_p^\times$ has index 2. This implies that K_g is the quadratic subfield of the p-th cyclotomic field, which is known to be $\mathbf{Q}(\sqrt{\pm p})$, where the sign is chosen such that $\pm p \equiv 1 \pmod 4$.

8.8 The ring $R(G)$

8.8.1. The ring of virtual characters.

A function $f : G \to \mathbf{C}$ is called a **virtual character**, or a **generalized character**, if it is the difference of two characters. This is equivalent to saying that

$$f = \sum_{\chi \in \mathrm{Irr}(G)} n_\chi \chi \quad \text{with } n_\chi \in \mathbf{Z}. \tag{8.13}$$

The set $R(G)$ of all virtual characters is a commutative ring; it is called the **representation ring** of G. It is $\mathbf{Z}$-free, with basis $\mathrm{Irr}(G)$.
The characters make up a subset of $R(G)$, closed under addition and multiplication, which we shall denote by $R_+(G)$.
There is a natural *involution* $f \mapsto f^*$ on $R(G)$, defined by :

$$f^*(g) = f(g^{-1}) = \overline{f(g)}.$$

Let $\mathcal{C}_G$ be the category of linear representations of G. The ring $R(G)$ may be viewed as the **Grothendieck group** of $\mathcal{C}_G$. This means that it has the following property:

Proposition 8.43. *Let Φ be an abelian group. For every object V of $\mathcal{C}_G$, let $\phi(V)$ be an element of Φ; assume that $\phi(V) = \phi(V') + \phi(V'')$ for every exact sequence*

$$0 \to V' \to V \to V'' \to 0.$$

Then there exists a unique homomorphism $\iota_\phi : R(G) \to \Phi$ such that $\iota_\phi(\chi_V) = \phi(V)$.

Proof. Indeed, ι_ϕ is characterized by its value for $\chi \in \mathrm{Irr}(G)$, which is $\phi(V_\chi)$.

Let us now compare $R(G)$ with another ring $R'(G)$ of class functions on G.

Proposition 8.44. *With the notation of §8.7, let $R'(G)$ be the ring of class functions on G with values in A_N such that $f(g^m) = \sigma_m(f(g))$ for every $g \in G$ and every integer m prime to $|G|$. Then :*
(1) We have $R(G) \subset R'(G)$.
(2) $f \in R'(G) \Longrightarrow |G|.f \in R(G)$.

Proof of (1). This follows from part (3) of th.8.41.

Proof of (2). Let us write $|G|.f$ as a linear combination $\sum c_\chi \chi$ of irreducible characters. We need to prove that c_χ belongs to $\mathbf{Z}$ for every χ. We have $c_\chi = \sum_{g \in G} f(g)\chi(g^{-1})$. This shows that c_χ belongs to A_N. Moreover, if m is prime to $|G|$, we have

$$\sigma_m(c_\chi) = \sum_g f(g^m)\chi(g^{-m}) = c_\chi,$$

since $g \mapsto g^m$ is a bijection of G onto G. Hence c_χ is invariant by the Galois group Σ_N, which means that it belongs to $\mathbf{Q}$; since it is an algebraic integer, it belongs to $\mathbf{Z}$.

Corollary 8.45. *$R(G)$ has finite index in $R'(G)$.*

Proof. This follows from (1) and (2).

Remark. When $G \neq 1$, the rings $R(G)$ and $R'(G)$ are distinct. Indeed, the function f defined by $f(1) = 1$ and $f(g) = 0$ if $g \neq 1$ belongs to $R'(G)$ but not to $R(G)$. More precisely, if $a \in \mathbf{Z}$, the function af belongs to $R(G)$ if and only if a is divisible by $|G|$; this shows that the index of $R(G)$ in $R'(G)$ is divisible by $|G|$.

8.8.2. Adams operations.

Let $m \in \mathbf{Z}$. If f is a function on G, let us denote by $\Psi^m f$ the function $g \mapsto f(g^m)$. The Ψ^m are the **Adams operations**. They are linear, multiplicative, and they satisfy the identities:

- $\Psi^{mm'} = \Psi^m \circ \Psi^{m'}$.
- $\Psi^0 f = f(1).1$.
- $\Psi^1 f = f$.
- $\Psi^{-1} f = f^* = \{g \mapsto f(g^{-1})\}$.

Moreover:

Theorem 8.46. *If $f \in R(G)$, then $\Psi^m f \in R(G)$ for every $m \in \mathbf{Z}$.*

Proof. The formulas above show that it is enough to prove this when m is > 0. Since Ψ^m is linear, we may also assume that f is the character of a linear representation ρ of G; let $n = f(1)$ be the degree of ρ.
Let $P(X_1, \ldots, X_n)$ be a symmetric polynomial in n indeterminates $(X_1, \ldots, X_n)$. If $g \in G$, and if $(\lambda_1, \ldots, \lambda_n)$ are the eigenvalues of $\rho(g)$, put $f_P(g) = P(\lambda_1, \ldots, \lambda_n)$; since P is symmetric, this does not depend on the numbering of the λ_i. When P is the polynomial $\sum X_i^m$, f_P is equal to $\Psi^m f$. Hence, th.8.46 is a special case of the following:

Theorem 8.47. *We have $f_P \in R(G)$ if the coefficients of P belong to $\mathbf{Z}$.*

Proof of theorem 8.47. Consider first the case where P is an elementary symmetric polynomial $S_k = \sum_{i_1 < \cdots < i_k} X_{i_1} \cdots X_{i_k}$. In that case, $f_P(g)$ is the trace of $\wedge^k \rho(g)$, i.e., $f_P = \lambda^k f$, which is a character of G, cf. §8.1.4.
The general case follows: indeed, every symmetric polynomial with coefficients in $\mathbf{Z}$ belongs to $\mathbf{Z}[S_1, S_2, \ldots]$, cf. Bourbaki [4], IV-6, th.1, or Lang [29], IV, th.6.1, and, if th.8.47 is true for two polynomials, it is also true for their sum, their difference and their product.

Remarks.
1. The proofs above are those of Frobenius, [19], n°78, §8; they date from about 50 years before the Adams operations were introduced in K-theory.
2. If m is prime to $|G|$, the map Ψ^m is the conjugation map $f \mapsto \sigma_m(f)$, cf. th.8.41;

in particular, Ψ^m is an automorphism of $R(G)$ and it maps $R_+(G)$ onto itself. These properties do not hold for arbitrary m's, cf. exerc.13.
3. The proof of th.8.46 gives an explicit method to compute the Ψ^m from the λ^k, and vice-versa. All one has to do is to write the polynomial $P_m = \sum X_i^m$ as a polynomial in $S_1, \ldots, S_m$. For instance:

- The formula $P_2 = S_1^2 - 2S_2$ gives $\Psi^2 f = f^2 - 2\lambda^2 f$, cf. prop.8.1 (7).
- The formula $P_3 = S_1^3 - 3S_1S_2 + 3S_3$ gives $\Psi^3 f = f^3 - 3f.\lambda^2 f + 3\lambda^3 f$.

For larger values of m, one may use a recursion based on *Newton formulas* (Bourbaki [4], IV-6, lemma 4):

$$\Psi^m f = \sum_{k=1}^{m-1} (-1)^{k-1} \lambda^k f . \Psi^{m-k} f + (-1)^{m+1} m \lambda^m f, \quad m \geqslant 2. \tag{8.14}$$

See also exerc.20.

8.9 Realizing representations over a subfield of C, for instance the field R

8.9.1. A realizability criterion.

Let V be a linear representation of G of degree n, and let χ be its character. If k is a subfield of $\mathbf{C}$ containing the values of χ, let us say that V is **realizable over** k if there exists a k-linear representation V_0 of G such that $V \simeq \mathbf{C} \otimes_k V_0$, i.e., if there exists a homomorphism $\rho_0 : G \to \mathrm{GL}_n(k)$ with character χ.

[In that case, V_0 is unique, up to $k[G]$-isomorphisms: this follows from a general result on scalar extensions for finite-dimensional modules, cf. Bourbaki [5], §2, th.3.]

Let us consider the case where V is *irreducible*; let $\chi \in \mathrm{Irr}(G)$ be its character, and let $n = \dim V$ be its degree. As in §8.5 let us denote by

$$r_\chi : \mathbf{C}[G] \to \mathrm{End}(V) \quad \text{and} \quad \rho_\chi : G \to \mathrm{GL}(V)$$

the corresponding homomorphisms; let $\epsilon_\chi \in \mathbf{C}[G]$ be the central idempotent associated to χ, cf. formula (8.8); its image in $\mathrm{End}(V)$ is id_V. Since we assume that k contains the values of χ, we have $\epsilon_\chi \in k[G]$. Hence $k[G]$ splits as the direct sum of the two-sided ideals generated by $1 - \epsilon_\chi$ and ϵ_χ:

$$k[G] = (1 - \epsilon_\chi)k[G] \ \oplus \ \epsilon_\chi k[G]; \tag{8.15}$$

this gives a direct product decomposition of the algebra $k[G]$:

$$k[G] = A_\chi \times B_\chi, \tag{8.16}$$

with $A_\chi = k[G]/(1 - \epsilon_\chi)k[G]$ and $B_\chi = k[G]/\epsilon_\chi k[G]$.

After tensoring (8.16) by $\mathbf{C}$, we obtain by th.8.5 the decomposition of $\mathbf{C}[G]$:

$$\mathbf{C}[G] = \mathrm{End}(V) \times \prod_{\chi' \neq \chi} \mathrm{End}(V_{\chi'}). \tag{8.17}$$

This implies that $\mathbf{C} \otimes_k A_\chi \to \mathrm{End}(V)$ is an isomorphism; hence $\dim A_\chi = n^2$. We may view A_χ as the k-subalgebra of $\mathrm{End}(V)$ generated by $\rho_\chi(G)$.

Theorem 8.48. *Assume that k contains the values of χ. The following properties are equivalent :*
(1) The representation V is realizable over k.
(2) The k-algebra A_χ is isomorphic to the matrix algebra $\mathrm{M}_n(k)$.
(3) There exists $\alpha \in A_\chi$ such that $\dim_k A_\chi/A_\chi\alpha = n$.
(4) There exists $a \in k[G]$ with $\dim \mathrm{Ker}\ a_V = 1$, where a_V denotes the endomorphism $x \mapsto ax$ of V.

We shall use the following lemma on the left ideals of a matrix ring:

Lemma 8.49. *Let E be a vector space of dimension n over a field F. If $u \in \mathrm{End}(E)$ has rank r, then $\dim \mathrm{End}(E)u = nr$.*

Proof of lemma 8.49. Let $N \subset E$ be the kernel of u. Every element v of the ideal $\mathrm{End}(E)u$ vanishes on N. Conservely, if v has that property, it can be factored as $v = w \circ u'$, where $u' : E \to \mathrm{Im}\ u$ is defined by u and w is a linear map of $\mathrm{Im}\ u$ into V; by extending w to V we obtain $z \in \mathrm{End}(V)$ such that $v = zu$. This shows that $\mathrm{End}(E)u$ is isomorphic to $\mathrm{Hom}(E/N, E)$; its dimension over F is $n.\dim(E/N) = nr$.

Proof of theorem 8.48.

(1) $\Longrightarrow$ (2). If $V_0 \subset V$ is a k-realization of V, it is stable by $k[G]$, hence by A_χ. This defines an injective map $A_\chi \to \mathrm{End}_k(V_0)$; since both rings have dimension n^2, this map is an isomorphism. Hence $A_\chi \simeq \mathrm{End}_k(V_0) \simeq \mathrm{M}_n(k)$.

(2) $\Longrightarrow$ (3). Lemma 8.49, applied to $A_\chi \simeq \mathrm{M}_n(k)$ with $r = n-1$, shows that A_χ contains an element α such that $\dim_k A_\chi\alpha = n(n-1)$, hence $\dim_k A_\chi/A_\chi\alpha = n$.

(3) $\Longrightarrow$ (4). Let $\alpha \in A_\chi$ be such that $\dim_k A_\chi\alpha = n(n-1)$. Let a be an element of $k[G]$ whose image in A_χ is α. We have

$$\mathbf{C} \otimes_k A_\chi\alpha \simeq \mathrm{End}(V)a_V, \tag{8.18}$$

hence $\dim_{\mathbf{C}} \mathrm{End}(V)a_V = n(n-1)$. Lemma 8.49, applied to $F = \mathbf{C}, E = V, u = a_V$, shows that a_V has rank $n-1$, i.e., that $\dim \mathrm{Ker}\ a_V = 1$.

(4) $\Longrightarrow$ (1). Let $a \in k[G]$ be as in (4). Let x be a nonzero element of $\mathrm{Ker}\ a_V$ and let $V_0 = k[G]x = A_\chi x$. The map $\mathbf{C} \otimes_k V_0 \to V$ is surjective, since its image is nonzero and is $\mathbf{C}[G]$-stable; hence $\dim_k V_0 \geqslant n$. On the other hand, since $a_V x = 0$, V_0 is a quotient of $A_\chi/A_\chi a_V$. Formula (8.18) shows that $\dim_k A_\chi a_V = \dim_{\mathbf{C}} \mathrm{End}(V)a_V$, which is equal to $n(n-1)$ by lemma 8.49. Hence $\dim_k V_0 \leqslant \dim_k A_\chi/A_\chi a_V = n$. This shows that $\dim_k V_0 = n$ and that $\mathbf{C} \otimes_k V_0 \to V$ is an isomorphism. Hence V_0 is a k-realization of V.

Corollary 8.50. *Suppose that there exist $g \in G$ and $\lambda \in k$ such that λ is an eigenvalue of g_V of multiplicity 1. Then V is realizable over k.*

Proof. This follows from th.8.48 applied to $a = g - \lambda$.

[Note that the proof gives an explicit construction of a k-realization of V, namely the $k[G]$-submodule of V generated by a nonzero eigenvector of g_V with eigenvalue λ.]

8.9.2. Realizability over R : Frobenius-Schur's theorem.

In the case $k = \mathbf{R}$, there is a simple realizability criterion, due to Frobenius and Schur (Frobenius, [19], n°75):

Theorem 8.51. *A linear representation V of G is realizable over* **R** *if and only if there exists a nondegenerate symmetric bilinear form on V which is G-invariant.*

[Note that the existence of an invariant nondegenerate bilinear form on V means that V is isomorphic to its dual, hence (cf. cor.8.7) that its character is **R**-valued. The main point of the theorem is that *the bilinear form should be symmetric.* Alternating bilinear forms correspond to quaternionic representations, cf. exerc.18.]

Proof. If V is of the form $V_0 \otimes_{\mathbf{R}} \mathbf{C}$, where V_0 is an **R**-representation of G, let $B_0(x, y)$ be a symmetric **R**-bilinear form on V_0, which is positive definite, i.e., such that $B_0(x, x) > 0$ for every $x \in V_0 - \{0\}$. Let $B(x, y) = \sum_{g \in G} B_0(gx, gy)$; then B is positive definite, hence nondegenerate, and G-invariant. By scalar extension from **R** to **C** we obtain a G-invariant nondegenerate symmetric bilinear form on V.

It remains to prove the converse, i.e., that the existence of such a bilinear form implies the existence of V_0. Let us prove first :

Proposition 8.52. *Let E be a finite dimensional vector space over* **C**. *Let $h(x, y)$ be a positive definite hermitian form on E and let $B(x, y)$ be a nondegenerate symmetric bilinear form on E. Then there exists an* **R**-*vector subspace E_0 of E such that :*
(1) $E = E_0 \oplus iE_0$;
(2) $gE_0 = E_0$ *for every $g \in \mathrm{GL}(V)$ which fixes h and B.*

Proof of prop.8.52.
Let us write $h(x, y)$ as $\langle x, y\rangle$. For every $y \in E$, the map $x \mapsto B(x, y)$ is linear; hence there exists $\varphi(x) \in E$ such that $B(x, y) = \langle \varphi(x), y\rangle$. The map $\varphi : E \to E$ so defined is antilinear (i.e., such that $\varphi(\lambda x) = \overline{\lambda}\varphi(x)$) and bijective. Since B is symmetrical, we have :

$$\langle \phi(x), y\rangle = \langle \phi(y), x\rangle. \tag{8.19}$$

Hence :

$$\langle \phi^2(x), y\rangle = \langle \phi(y), \phi(x)\rangle. \tag{8.20}$$

In particular, we have

$$\langle \phi^2(x), x\rangle = \langle \phi(x), \phi(x)\rangle > 0 \text{ if } x \neq 0. \tag{8.21}$$

Hence ϕ^2 is a *positive hermitian* linear automorphism of E, in the sense of §9.2.2.

Corollary 9.11, applied to $a = \phi^2$, shows[4] that there exists a unique positive hermitian automorphism b such that $b^2 = \phi^2$. If $b' = \phi b \phi^{-1}$, b' has the same property as b with respect to $\phi\phi^2\phi^{-1} = \phi$. By the uniqueness of b, this shows that $b' = b$, i.e., that b and ϕ commute. Let $\sigma = \phi b^{-1}$; we have $\sigma^2 = \phi^2 b^{-2} = 1$; moreover, σ is antilinear. The vector space E splits as $E = E_0 \oplus F$, where E_0 (resp. F) is the space of $x \in E$ such that $\sigma x = x$ (resp. $\sigma x = -x$). The antilinearity of σ implies that $F = iE_0$. We thus have an E_0 with property (1) of prop.8.52. As for property (2) it follows from the fact that the construction is canonical; hence, if g fixes both the hermitian form h and the bilinear form B, it commutes with ϕ, b and σ and it maps E_0 onto itself.

End of the proof of th.8.51. Suppose that V has an invariant nondegenerate G-invariant symmetric bilinear form. Choose a G-invariant positive definite hermitian form h on V. By prop.8.52, there exists $V_0 \subset V$ which is G-invariant and such that $V = V_0 \oplus iV_0$, i.e., $V \simeq V_0 \otimes_{\mathbf{R}} \mathbf{C}$; hence V_0 is the required $\mathbf{R}$-representation of G.

8.9.3. Realizability over R : irreducible representations.

The following consequence of th.8.51 is also due to Frobenius and Schur ([19], n°75):

Theorem 8.53. *Let V be an irreducible representation of G, and let χ be its character. There are three different possibilities :*
(1) $\langle \Psi^2\chi, 1\rangle = 0$; the character χ is not real valued ; the only G-invariant bilinear form on V is 0.
(2) $\langle \Psi^2\chi, 1\rangle = 1$; the character χ is real valued ; there exists a G-invariant nonzero symmetric bilinear form on V; the representation V is realizable over $\mathbf{R}$.
(3) $\langle \Psi^2\chi, 1\rangle = -1$; the character χ is real valued ; there exists a G-invariant nonzero alternating bilinear form on V; the representation V is not realizable over $\mathbf{R}$.

[Recall that $\Psi^2\chi$ is the virtual character $g \mapsto \chi(g^2)$, cf. §8.8.2. The scalar product $\langle \Psi^2\chi, 1\rangle$ is thus equal to $\frac{1}{|G|}\sum_{g\in G}\chi(g^2)$.]

Proof. If $\chi \neq \overline{\chi}$, V is not isomorphic to its dual V^*, hence $\mathrm{Hom}_G(V, V^*) = 0$, which means that the only G-invariant bilinear form over V is 0. We have $\langle \chi, \overline{\chi}\rangle = 0$, i.e., $\langle \chi^2, 1 >= 0$, i.e., $(V \otimes V)^G = 0$. Since $V \otimes V = \wedge^2 V \oplus \mathrm{Sym}^2 V$, this implies $(\wedge^2 V)^G = 0$ and $(\mathrm{Sym}^2 V)^G = 0$. If we denote by $\lambda^2\chi$ and $\sigma^2\chi$ the characters of $\wedge^2 V$ and $\mathrm{Sym}^2 V$, we have $\langle \lambda^2\chi, 1\rangle = 0 = \langle \sigma^2\chi, 1\rangle$. By prop.8.1, $\Psi^2\chi = \sigma^2\chi - \lambda^2\chi$, hence $\langle \Psi^2\chi, 1\rangle = 0$. This is case (1).

Suppose now that $\chi = \overline{\chi}$, i.e., $V \simeq V^*$. The space of G-invariant bilinear form on V is isomorphic to $(V^* \otimes V^*)^G \simeq (V \otimes V^*)^G \simeq \mathrm{Hom}_G(V, V)$, hence is 1-dimensional. This

[4] We are using here a result proved in the next chapter. The reader can check that this does not lead to a vicious circle.

means that there exists a nonzero G-invariant bilinear form B on V, which is unique, up to scalar multiplication. The form B is nondegenerate: otherwise its kernel would be a nonzero proper G-stable subspace of V, contradicting the fact that V is irreducible. The essential uniqueness of B shows that B is either symmetric or alternating.
If B is symmetric, we have $\langle \lambda^2\chi, 1\rangle = 0$ and $\langle \sigma^2\chi, 1\rangle = 1$, hence $\langle \Psi^2\chi, 1\rangle = 1$. By th.8.51, V is realizable over $\mathbf{R}$. This is case (2).
If B is alternating, we have $\langle \lambda^2\chi, 1\rangle = 1$ and $\langle \sigma^2\chi, 1\rangle = 0$, hence $\langle \Psi^2\chi, 1\rangle = -1$. By th.8.51, V is not realizable over $\mathbf{R}$. This is case (3).

Examples of the three cases of th.8.53.

• Case (1). Take G cyclic of order 3, and $\chi \neq 1$.
More generally, if G had odd order, and $\chi \in \mathrm{Irr}(G)$ is $\neq 1$, then χ is not real valued (Burnside, cf. exerc.4).
• Case (2). All the irreducible representations of a symmetric group $\mathcal{S}_n$ can be realized over $\mathbf{Q}$, hence over $\mathbf{R}$: this follows from their construction in terms of partitions, see e.g. Fulton-Harris [20], §4.2. The same is true for all the Weyl groups.
• Case (3). The smallest example is that of the quaternion group $Q = \{\pm 1, \pm i, \pm j, \pm k\}$, and of its degree 2 irreducible complex representation.
Here $\chi(g) = 2$ when $g = 1$, $\chi(g) = -2$ when $g = -1$, and $\chi(g) = 0$ otherwise. Hence $\langle \Psi^2\chi, 1\rangle = (2 + 2 - 2.6)/8 = -1$. The corresponding algebra A_χ (over $k = \mathbf{R}$) is the quaternion skewfield; since it is a division algebra, it is not isomorphic to a matrix algebra.

8.10 Application of character theory: proof of Frobenius's theorem 6.7

Recall the statement (cf. §6.3):

Let H be a subgroup of G such that $H \cap gHg^{-1} = 1$ for all $g \in G - H$. Let N be the set of elements of G that are, either equal to 1, or not conjugate to any element of H. Then:

Theorem 8.54. *The set N is a subgroup of G.*

Strategy of the proof. The main step consists in showing that *every linear representation of H can be extended to G in such a way that it is trivial on N*; this will be done by extending the character of the representation from H to G and proving that the function so obtained is a character of G.

Proof.

We start by extending to G any class function on H:

Lemma 8.55. *Let f be a class function on H. There exists a unique class function $\widetilde{f}$ on G which extends f and is constant on N.*

Proof. The uniqueness of $\widetilde{f}$ follows from the fact that every conjugacy class of G either meets H, or is contained in N. Let us prove the existence. If $x \in N$, we put $\widetilde{f}(x) = f(1)$. If $x \notin N$, we write x in the form ghg^{-1}, with $g \in G$, $h \in H - \{1\}$, and we put $\widetilde{f}(x) = f(h)$. This does not depend on the choices of g and h: indeed, if $g'h'g'^{-1} = ghg^{-1}$, we have $g'^{-1}g.h.g^{-1}g' = h'$, hence $g'^{-1}g \in H$; this shows that h and h' are conjugate in H; since f is a class function, we have $f(h) = f(h')$.

In what follows, we use $\langle \alpha, \beta \rangle_G$ to denote the scalar product $\frac{1}{|G|}\sum_{g\in G} \alpha(g^{-1})\beta(g)$ on the group G. Similarly, $\langle \alpha, \beta \rangle_H$ denotes the scalar product on H.

Lemma 8.56. *Let f and $\widetilde{f}$ be as in lemma 8.55, and let θ be a class function on G; let θ_H be the restriction of θ to H. Then :*

$$\langle \widetilde{f}, \theta \rangle_G = \langle f, \theta_H \rangle_H + f(1)\langle 1, \theta \rangle_G - f(1)\langle 1, \theta_H \rangle_H. \tag{8.22}$$

Proof. Equation (8.22) holds if $f = 1$, since then $\widetilde{f} = 1$. Hence, we only need to prove it when $f(1) = 0$, in which case the formula reduces to :

$$\langle \widetilde{f}, \theta \rangle_G = \langle f, \theta_H \rangle_H. \tag{8.23}$$

Let $\mathcal{R}$ be a set of representatives of the left cosets of H. As r runs through $\mathcal{R}$, rHr^{-1} runs through all of the conjugates of H; and every element $\neq 1$ of a conjugate of H can be written uniquely as rhr^{-1} with $r \in \mathcal{R}$ and $h \in H$. Since $\widetilde{f}$ is zero outside the union of the conjugates of H, we have:

$$\begin{aligned}\langle \widetilde{f}, \theta \rangle_G &= \tfrac{1}{|G|}\textstyle\sum_{(r,h)\in\mathcal{R}\times H} \widetilde{f}(rhr^{-1})\theta(h^{-1}) = \tfrac{|\mathcal{R}|}{|G|}\sum_{h\in H} f(h)\theta(h^{-1}) \\ &= \tfrac{1}{|H|}\textstyle\sum_{h\in H} f(h)\theta(h^{-1}) = \langle f, \theta_H \rangle_H.\end{aligned}$$

Lemma 8.57. *The map $f \mapsto \widetilde{f}$ is an isometry, i.e., $\langle \widetilde{f_1}, \widetilde{f_2} \rangle_G = \langle f_1, f_2 \rangle_H$ for every class functions f_1 and f_2 on G.*

Proof. Equation (8.22), applied to $\theta = 1$, shows that $\langle \widetilde{f}, 1 \rangle_G = \langle f, 1 \rangle_H$.

Define f_2^* by $f_2^*(g) = f_2(g^{-1})$. We have :

$$\langle \widetilde{f_1}, \widetilde{f_2} \rangle_G = \langle \widetilde{f_1}\widetilde{f_2^*}, 1 \rangle_G = \langle \widetilde{f_1 f_2^*}, 1 \rangle_G = \langle f_1 f_2^*, 1 \rangle_H = \langle f_1, f_2 \rangle_H.$$

Lemma 8.58. *If f is a character of H and θ is a character of G, then $\langle \widetilde{f}, \theta \rangle_G$ is an integer.*

Proof. Since θ is a character of G, its restriction θ_H to H is a character of H, hence every term on the right side of equation (8.22) is an integer.

Lemma 8.59. *If χ is an irreducible character of H, then $\widetilde{\chi}$ is an irreducible character of G.*

Proof. Let $\theta_1, \ldots, \theta_m$ be the irreducible characters of G. Since $\widetilde{\chi}$ is a class function, we have $\widetilde{\chi} = \sum c_i\theta_i$, with $c_i \in \mathbf{C}$. Lemma 8.58 shows that the c_i are integers. We have $\sum c_i^2 = \langle \widetilde{\chi}, \widetilde{\chi}\rangle_G = \langle \chi, \chi\rangle_H = 1$, hence all the c_i are 0 except one of them, say c_j, which is ± 1. If c_j were equal to -1, we would have $\widetilde{\chi} = -\theta_j$. But $\widetilde{\chi}(1) = \chi(1) > 0$ and $\theta_j(1) > 0$, hence this is impossible. Thus, $c_j = 1$, i.e., $\widetilde{\chi} = \theta_j$.

Lemma 8.60. *If χ is a character of H, then $\widetilde{\chi}$ is a character of G.*

Proof. This follows from lemma 8.59 by writing χ as a sum of irreducible characters.

End of the proof of th.8.54. Choose a representation ρ of H with trivial kernel, for instance the regular representation. Let χ be the character of ρ; by lemma 8.60, there exists a representation $\widetilde{\rho}$ of G with character $\widetilde{\chi}$. If $g \in G$ is conjugate to an element h of $H - \{1\}$, we have $\widetilde{\chi}(g) = \chi(h) \neq \chi(1) = \widetilde{\chi}(1)$, hence $\widetilde{\rho}(g) \neq 1$. If $g \in N$, we have $\widetilde{\chi}(g) = \chi(1) = \widetilde{\chi}(1)$, hence $\widetilde{\rho}(g) = 1$, cf. prop.8.5 (4). Therefore, $N = \mathrm{Ker}\ \widetilde{\rho}$, which implies that N is a subgroup of G.

Remark. The proof given here can be shortened by using *induced characters*, cf. exerc.34.

8.11 Application of character theory: proof of Burnside's theorem 5.4

We keep the notation of §8.6 and §8.7.

Proposition 8.61. *Let g be an element of $G - \{1\}$ and let $c(g)$ be the number of elements of the conjugacy class of g. Suppose that $c(g)$ is a power of a prime p. Then there exists a normal subgroup N of G, different from G, such that the image of g in G/N belongs to the center of G/N.*

Proof. By part (3) of th.8.21 we have $\sum_{\chi\in\mathrm{Irr}(G)} \chi(1)\chi(g) = 0$. Therefore,

$$\sum_{\chi\neq 1} \frac{\chi(1)\chi(g)}{p} = -\frac{1}{p}.$$

Since $-\frac{1}{p}$ is not an algebraic integer, there exists $\chi \in \mathrm{Irr}(G)$, with $\chi \neq 1$, such that $\chi(1)\chi(g)/p$ is not an algebraic integer. In particular, $\chi(g)$ is $\neq 0$ and p does not divide $\chi(1)$, hence $c(g)$ and $\chi(1)$ are relatively prime. By part (3) of prop.8.37, if ρ_χ is a representation of G of character χ, then $\rho_\chi(g)$ is a homothety. The kernel N of ρ_χ is a proper normal subgroup of G. We have $G/N \simeq \mathrm{Im}(\rho_\chi)$; the fact that $\rho_\chi(g)$ is a homothety implies that the image of g in G/N belongs to the center of G/N.

We now prove :

Theorem 8.62 (Burnside). *Every group G of order $p^a q^b$ (where p and q are primes) is solvable.*

Proof. Use induction on $|G|$. We may assume that G is a simple group, and also that b is nonzero (otherwise G is a p-group). If $g \in G$, denote by $c(g)$ the number of elements of the conjugacy class of g. There exists $g \in G - \{1\}$ such that q does not divide $c(g)$, otherwise we would have $|G| \equiv 1 \pmod{q}$. Let g be such an element. Since $c(g)$ divides $p^a q^b$, it is a power of p. By prop.8.61, there exists a proper normal subgroup N of G such that the image of g in G/N lies in the center of G/N. Since G is simple, we have $N = 1$, hence g belongs to the center of G. Since G is simple, this shows that G is cyclic.

8.12 The character table of $\mathcal{A}_5$

As an example of construction of character tables, we give the case $G = \mathcal{A}_5$.

8.12.1. The degrees of the irreducible characters.

The *conjugacy classes* of G are as follows.

The elements of order 1 (resp. 2, 3) make up one class of size 1 (resp. 15, resp. 20), which have representatives : $1A = 1, 2A = (1\ 2)(3\ 4), 3A = (1\ 2\ 3)$.
The elements of order 5 make up two classes of 12 elements each, with representatives $5A = (1\ 2\ 3\ 4\ 5)$, and $5B =$ square of 5A. (Note that the normalizer of a 5-Sylow subgroup acts on that group by $z \mapsto z^{\pm 1}$.)
The classes of 1A, 2A, 3A are rational (in the sense of §8.7.3). The classes of 5A and 5B are real but not rational; their field of rationality is the quadratic subfield of $\mathbf{Q}(\mu_5)$, that is $\mathbf{Q}(\sqrt{5})$.

Since there are 5 conjugacy classes, there are 5 irreducible characters, $\chi_1, \ldots, \chi_5$. We label them in such a way that their degrees a, b, c, d, e are such that $a \leqslant b \leqslant c \leqslant d \leqslant e$. We have

$$a^2 + b^2 + c^2 + d^2 + e^2 = 60. \tag{8.24}$$

Let us determine a, b, c, d, e :

• We have $a = 1$, $\chi_1 = 1$ and there is no other irreducible character of degree 1, since $G^{\mathrm{ab}} = 1$.

• There is no irreducible character of degree 2: if there was an embedding $G \to \mathrm{GL}_2(\mathbf{C})$, the group G would be contained in $\mathrm{SL}_2(\mathbf{C})$ because $G^{\mathrm{ab}} = 1$; since the only element of order 2 of $\mathrm{SL}_2(\mathbf{C})$ is -1, this is impossible.

• We have $b = 3$: otherwise b^2, c^2, d^2, e^2 would be $\geqslant 16$ which would contradict (8.24). If $\rho : G \to \mathrm{GL}_3(\mathbf{C})$ is an irreducible representation with character χ_2, the eigenvalues of $\rho(5A)$ contain at least one primitive 5th-root of unity z; since the inverse of $5A$ is

conjugate to $5A$, z^{-1} is also an eigenvalue, and the third eigenvalue is 1 because $\rho(G)$ is contained in $\mathrm{SL}_3(\mathbf{C})$; we have $\chi_2(5A) = 1 + z + z^{-1} = (1 \pm \sqrt{5})/2$, which belongs to $\mathbf{Q}(\sqrt{5})$ but not to $\mathbf{Q}$. If we denote by σ the automorphism $\sqrt{5} \mapsto -\sqrt{5}$ of $\mathbf{Q}(\sqrt{5})$, the character $\sigma(\chi_2)$ is another degree 3 character (cf. th.8.41), which we may choose as χ_3. We thus have $c = 3$.

• We have $d^2 + e^2 = 60 - 1 - 9 - 9 = 41$. There is only one decomposition of 41 as a sum of two squares[5], namely $41 = 16 + 25$. Hence $d = 4$ and $e = 5$.

8.12.2. The values of the irreducible characters.

Values of χ_2. The eigenvalues of $2A$ are equal to 1 or -1; they cannot all be 1, and their product is 1; the only possibility is $1, -1, -1$, hence $\chi_2(2A) = -1$. The eigenvalues of $3A$ contain at least one primitive 3rd-root of unity w; since the class of $3A$ is rational, w^{-1} is also an eigenvalue; since the product of the eigenvalues is 1, the three eigenvalues are $1, w, w^{-1}$, hence $\chi_2(3A) = 0$. We have already seen that $\chi_2(5A) = (1 \pm \sqrt{5})/2$. We may label χ_2 and χ_3 in such a way that $\chi_2(5A)$ is equal to $t = (1 + \sqrt{5})/2$; then $\chi_2(5B)$ is equal to its Galois conjugate $t' = (1 - \sqrt{5})/2$.

Values of χ_3. For $1A, 2A, 3A$, they are the same as those of χ_2, since $\chi_3 = \sigma(\chi_2)$. We have $\chi_3(5A) = t'$ and $\chi_3(5B) = t$.

Values of χ_4. The eigenvalues of $2A$ are $1, 1, -1, -1$: if not, since their product is 1, they would be $1, 1, 1, 1$ or $-1, -1, -1, -1$ which are both impossible; hence $\chi_4(2A) = 0$. The eigenvalues of $3A$ are either $1, 1, w, w^{-1}$ or w, w, w^{-1}, w^{-1}, hence $\chi_4(3A) = 1$ or -2. The eigenvalues of $5A$ are the four primitive 5-roots of unity, otherwise $\chi_4(5A)$ would not be rational, and there would be another irreducible character of degree 4; hence $\chi_4(5A) = -1$ and the same is true for $5B$. The equation $\sum_{g \in G} \chi_4(g) = 0$ gives :

$$1.4 + 15.0 + 20.\chi_4(3A) + 24.(-1) = 0,$$

hence $\chi_4(3A) = 1$.

Values of χ_5. The formula

$$\sum_{i=1}^{5} \chi_i(1)\chi_i(g) = 0 \ \text{ if } g \neq 1, \tag{8.25}$$

gives : $\chi_5(2A) = 1, \chi_5(3A) = -1, \chi_5(5A) = \chi_5(5B) = 0$.

[*Alternative method.* Once χ_2 has been computed, one may recover the other characters by splitting its powers. For instance, let $f = \chi_2^2$. One finds that $\langle f, \chi_2 \rangle = \langle f, 1 \rangle = 1, \langle f, f \rangle = 3$, hence f splits as $f = 1 + \chi_2 + \psi$, where ψ is irreducible of degree 5, hence is the character χ_5.]

We thus obtain the following table:

[5] This is a general property of prime numbers which are $\equiv 1 \pmod 4$.

characters	60	4	3	5	5	← orders of centralizers
↓	$1A$	$2A$	$3A$	$5A$	$5B$	← representatives of the conjugacy classes
χ_1	1	1	1	1	1	
χ_2	3	-1	0	t	t'	$\leftarrow t = \frac{1+\sqrt{5}}{2}, \ t' = \frac{1-\sqrt{5}}{2}$
χ_3	3	-1	0	t'	t	
χ_4	4	0	1	-1	-1	
χ_5	5	1	-1	0	0	

Remark. Note the five zeros in the table. That there is at least one zero for every χ_i of degree > 1 is a general result of Burnside (see exerc.25). The following theorem of Brauer (cf. [37], §16.4, cor. to prop.46) gives another such information:

Let G be a finite group, p a prime number, $g \in G$ and $\chi \in \mathrm{Irr}(G)$. Assume that p does not divide $|G|/\chi(1)$ and that p divides the order of g. Then $\chi(g) = 0$.

By applying this to the triplets $(2, 2A, \chi_4), (3, 3A, \chi_2), (3, 3A, \chi_3), (5, 5A, \chi_5), (5, 5B, \chi_5)$, all the zeros of the table are explained.

8.12.3. Description of the irreducible representations.

Degree 3 representations. A regular icosahedron in $\mathbf{R}^3$ has for automorphism group the group $\{\pm 1\} \times G$. This gives an embedding $G \to \mathrm{SO}_3(\mathbf{R})$. If one chooses the coordinates in such a way that the 12 vertices are $(0, \pm 1, \pm t)$, $(\pm 1, \pm t, 0)$, $(\pm t, 0, \pm 1)$, the matrices representing the elements of G have their coefficients in $\mathbf{Q}(t) = \mathbf{Q}(\sqrt{5})$. The two embeddings of that field in $\mathbf{R}$ (and hence in $\mathbf{C}$) correspond to χ_2 and χ_3; we also see that the corresponding representations are realizable over $\mathbf{Q}(\sqrt{5})$ [this also follows from cor.8.50, applied with $\lambda = 1$, and g any element $\neq 1$].

Another way to see this is to view $\{\pm 1\} \times G$ as the group generated by three plane reflections in $\mathbf{R}^3$, the angles beween the corresponding planes being $\pi/2, \pi/3$ and $\pi/5$; this means that $\{\pm 1\} \times G$ is the *Coxeter group* whose graph is

$$\circ \overset{5}{-} \circ - \circ \, ,$$

cf. Bourbaki [9], chap.VI, §4, th.1.

Degree 4 representation. The permutation representation associated to the action of G on $\{1, 2, 3, 4, 5\}$ splits into the direct sum of the unit representation and a representation ρ_4 of degree 4; the representation ρ_4 is irreducible: this follows from the fact that the action of G is 2-transitive, cf. exerc.10; the character of ρ_4 is χ_4.

Degree 5 representation. Same as for degree 4, except that the permutation representation is now given by the action of G of its six 5-Sylow subgroups; that action is also 2-transitive.

The degree 4 and 5 representations can also be viewed as the *Steinberg representations* of $G = \mathrm{PSL}_2(\mathbf{F}_q)$, for $q = 4$ and 5 respectively.

Note that the permutation interpretation of χ_4 and χ_5 explains why their minimal value is -1 ; indeed, the minimal number of fixed points is 0, by th.6.2 (Jordan).

8.12.4. Applications of the character table.

A character table contains implicitly a lot of information about the corresponding group. It is especially valuable for very large groups, such as those in ATLAS [16], because their character tables are still of manageable size. For instance, the Mathieu group M_{24}, of order 244823040, has a character table of size merely 26×26; that table was already determined by Frobenius in 1904 ([19], p. 346).

Here is an example. Let g be an element of a finite group G. Let $N(g)$ be the number of $x, y \in G$ such that $g = xyx^{-1}y^{-1}$. How can one compute $N(g)$? A straightforward method would be to look at each pair (x, y) in turn. That would require 3600 computations for $G = \mathcal{A}_5$ and it would not be feasible for M_{24}. But the character table gives an easy solution, namely :

$$N(g) = |G| \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(g)}{\chi(1)}, \tag{8.26}$$

cf. exerc.27, d). In the case $G = \mathcal{A}_5$, one finds :

$$N(1A) = 300,\ N(2A) = 32,\ N(3A) = 63,\ N(5A) = N(5B) = 65.$$

Similar formulas exist for other problems, for instance that of counting, for given elements $z_1, \ldots, z_k$, the number $N(z_1, \ldots, z_k)$ of families $(g_1, \ldots, g_k)$ such that:

$$g_1 \cdots g_k = 1 \quad \text{and} \quad g_i \text{ is conjugate to } z_i \text{ for every } i.$$

The formula is :

$$N(z_1, \ldots, z_k) = \frac{1}{|G|} |Z_1| \cdots |Z_k| \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(z_1) \cdots \chi(z_k)}{\chi(1)^{k-2}}, \tag{8.27}$$

where Z_i is the conjugacy class of z_i, cf. exerc.27, e).

8.13 Exercises

In the exercises below, G is a finite group; the ground field is $\mathbf{C}$ unless otherwise stated.

1. (*Detecting characters via their restrictions to subgroups.*)
   a) Let H be a proper subgroup of G. Show that there exist two distinct characters of G which coincide on H.
   [Hint: use Jordan's theorem, cf. §6.1.]
   b) Let $G = \mathrm{GL}_n(\mathbf{F}_q)$, with $n = 2$ or 3. Show that there exist two proper subgroups A

and B of G such that, if two characters of G coincide on $A \cup B$, they are equal.
[Hint: take A cyclic of order $q^n - 1$, and choose for B the stabilizer of a line in $\mathbf{F}_q^n$.]
c) Same as b) for $G = \mathcal{A}_n$, with $n = 4, 5, 6, 7$.
[Hint: for $\mathcal{A}_7$, take $A \simeq \mathcal{S}_5$ and $B \simeq \mathrm{SL}_3(\mathbf{F}_2)$.]

2. Suppose that $G \neq 1$. Show the equivalence of the two properties:
a) G is simple.
b) $\chi(g) \neq \chi(1)$ for every irreducible character $\chi \neq 1$ and every $g \neq 1$.
[Hint: use part (4) of prop.8.5.]

3. (*Brauer's lemma.*)
Let X and Y be two finite G-sets with $|X| = |Y| = n$. Let $f : X \times Y \to \mathbf{C}$ be a map such that $f(gx, gy) = f(x, y)$ for every x, y, g. Assume that the $n \times n$ matrix $(f(x,y)_{x\in X, y\in Y})$ is invertible. Show that $\chi_X = \chi_Y$, i.e., that $|X^g| = |Y^g|$ for every $g \in G$.
[Hint: show that the matrix $(f(x, y))$ defines a G-isomorphism of V_X onto V_Y.]

4. (*Brauer-Burnside.*) Let $X = \mathrm{Irr}(G)$ and let Y be the set of conjugacy classes of G. Let s be an automorphism of G; it acts on X and Y.
a) Show that $|X^s = |Y^s|$.
[Hint: apply exerc.3 with G replaced by the cyclic group generated by s. Make s act on X by $x \mapsto x \circ s^{-1}$, and on Y by $y \mapsto s(y)$. Use for f the evaluation map $X \times Y \to \mathbf{C}$.]
b) Show that $|Y^s|$ is equal to the number of orbits of G acting on itself by $z \mapsto gzs(g)^{-1}$.
[Hint: let $g \in G$ and let $y(g) \in Y$ be its class; let $n(g)$ be the number of $z \in G$ such that $z = gzs(g)^{-1}$. Show that $n(g) = 0$ if $y(g)$ is not fixed by s, and that $n(g) = |Z_G(g)|$ otherwise. Use Burnside's lemma.]
c) The group Σ_N defined in §8.7 acts on both X and Y. Show that $|X^\sigma| = |Y^\sigma|$ for every $\sigma \in \Sigma_N$.
[Hint: same methof as for a).]
d) A conjugacy class c is called *real* if its elements are real, i.e., if $g \in c \Longrightarrow g^{-1} \in c$. Show that the number of such classes is equal to the number of real irreducible characters.
[Hint: apply c) to the complex conjugation automorphism σ_{-1}.]
e) Suppose that $|G|$ is odd. Show that the only real conjugacy class of G is $\{1\}$, and that the only real-valued irreducible character of G is the character 1.

5. (*The character table viewed as a matrix.*)
Let X, Y be as in exerc.4. If $\chi \in X$ and $c \in Y$, define $\chi(c)$ as $\chi(g)$ for every $g \in c$. The family $T = (\chi(c))_{\chi\in X, c\in Y}$ may be viewed as an $X \times Y$-matrix, with X as the set of lines, and Y as the set of columns. Define similarly the $X \times Y$-matrix $U = (\chi(c)/z(c)^{1/2})$, where $z(c) = |G|/|c|$; if $g \in c$, then $z(c) = |Z_G(g)|$.

a) Show that U is a unitary matrix, i.e., that $U\,{}^t\overline{U} = 1$, where $\overline{U}$ is the complex conjugate of U, and ${}^t\overline{U}$ is its transpose (which is a $Y \times X$-matrix).
[Hint: show that the (χ, χ')-entry of $U\,{}^t\overline{U}$ is equal to

$$\sum_c \chi(c)\overline{\chi'(c)}/z(c) = \frac{1}{|G|}\sum_{g\in G} \chi(g)\overline{\chi'(g)},$$

and apply the orthogonality formula of characters.]
b) Show, by using a), that ${}^t\overline{U}\,U = 1$. This is equivalent to:

$$\textstyle\sum_{\chi\in X} \chi(g)\overline{\chi(g')} = 0 \text{ if } g, g' \text{ are not conjugate, and } \sum_{\chi\in X} |\chi(g)|^2 = |Z_G(g)|.$$

c) The choice of a bijection $X \to Y$ transforms T and U into square matrices; it gives a meaning to $\det(T)$ and $\det(U)$; changing the bijection leaves invariant $\det(T)^2$ and $\det(U)^2$.
Show that $\det(T)^2 = \det(U)^2 . \prod_{c \in Y} z(c)$.
Use a) to prove that $|\det(U)| = 1$, hence $|\det(T)| = \prod_{c \in Y} z(c)^{1/2}$.
d) If $c \in Y$, let c^* be its image by $g \mapsto g^{-1}$. Let C be the $Y \times Y$-matrix representing the permutation $c \mapsto c^*$. Show that $\det(C) = (-1)^{b/2}$, where b is the number of non-real conjugacy classes of G, cf. exerc.4. Show that $TC = \overline{T}$ and $UC = \overline{U}$. Deduce that $\det(T)$ and $\det(U)$ are real if $b/2$ is even and are purely imaginary if $b/2$ is odd. Conclude that

$$\det(T)^2 = (-1)^{b/2} \prod_{c \in Y} z(c).$$

6. (*G-sets and permutation representations.*)
Let X, Y be two finite G-sets, and let V_X, V_Y be the corresponding representations.
a) Suppose that $V_X \simeq V_Y$ and G is cyclic. Show that $X \simeq Y$.
b) Suppose that G is not cyclic. Show that there exist X and Y with $V_X \simeq V_Y$ and $X \not\simeq Y$.
[Hint: use the fact that the number of conjugacy classes of subgroups of G is strictly larger than the dimension of the space of $\mathbf{Q}$-valued virtual characters.]
c) Construct an example of b) such that G acts transitively on X, and non transitively on Y.
[Hint: take $|G| = 4$ and $|X| = |Y| = 6$.]
d) Construct an example of b) such that G acts transitively on both X and Y.
[Hint: take $G = \mathrm{SL}_3(\mathbf{F}_2)$, viewed as the automorphism group of the projective plane X over $\mathbf{F}_2$; choose for Y the set of projective lines of X. To show that $V_X \simeq V_Y$, use exerc.3 with $f(x, y) = 0$ (resp. 1) if the line y contains x (resp. does not contain x).]

7. Let H_1 and H_2 be two subgroups of G which generate G. Let $H = H_1 \cap H_2$. Let V be a linear representation of G (over an arbitrary field). Show that:

$$\dim V^G + \dim V^H \geqslant \dim V^{H_1} + \dim V^{H_2}.$$

[Hint: use $V^G = V^{H1} \cap V^{H_2}$.]

8. (*Irreducible representations of direct products.*) Let E be an irreducible representation of a group Γ (finite or infinite), and let W be an irreducible representation of the finite group G.
a) Show that $E \otimes W$ is an irreducible representation of $\Gamma \times G$.
b) Show that every irreducible representation of $\Gamma \times G$ is isomorphic to some $E \otimes W$, as in a).
[Hint: if V is an irreducible representation of $\Gamma \times G$, show that V, viewed as a representation of G, is a direct sum of copies of some irreducible G-representation W. Write V as $E \otimes W$, where $E = \mathrm{Hom}_G(W, V)$, cf. (8.10); the group Γ acts on E; show that E is Γ-irreducible.]
c) When Γ is finite, give different proofs of a) and b), based on character formulas.
d) Extend a) and b) to the representations of any finite product of groups (finite or infinite) over an algebraically closed field of any characteristic.

9. Let (G, H) be a Frobenius pair, with Frobenius kernel N, and let V be a linear representation of G. Prove that :
$$\dim V - \dim V^N = |H|.(\dim V^H - \dim V^G).$$
[Hint: apply lemma 8.56 to $f = r_H$ and $\theta = \chi_V$.]
In particular, $\dim V^H \leqslant \frac{1}{|H|} \dim V$ if $V^G = 0$.

10. (*n-transitivity via characters.*) Let X be a finite G-set, let V_X be the corresponding representation and let χ_X be the character of V_X, cf. prop.8.2. If $|X| \geqslant 1$, V_X splits as the direct sum of the trivial representation, and another representation V_X^0; let $\alpha_X = \chi_X - 1$ be the character of V_X^0.
a) Suppose that $|X| \geqslant 2$ and that the action of G is transitive, i.e., $\langle 1, \alpha_X \rangle = 0$. Show the equivalence of :
(i) V_X^0 is irreducible.
(ii) $\langle 1, \alpha_X^2 \rangle = 1$.
(iii) The action of G on X is 2-transitive (cf. exerc.11 of chap.1).
b) Suppose that $|X| \geqslant 3$ and conditions (i), (ii), (iii) are fulfilled. Show that $\langle 1, \alpha_X^3 \rangle \geqslant 1$, with equality if and only if the action of G on X is 3-transitive (cf. exerc.13 of chap.1).
[Hint: rewrite the conditions on $\langle 1, \alpha_X^2 \rangle$ and $\langle 1, \alpha_X^3 \rangle$ in terms of χ_X, and use the two exercises mentionned above.]

11. (*Schur-Blichfeldt*, cf. [34], n°6.) Let $\rho : G \to \mathrm{GL}(V)$ be a representation of G with trivial kernel, and let χ be its character. Let $n = \dim V$. Let Ω be the set of all $\chi(g)$, for $g \in G - \{1\}$, and let $P = \prod_{\omega \in \Omega}(n - \omega)$.
a) Show that P is real > 0.
[Hint: use that Ω is stable under complex conjugation, and that $\omega < n$ if $\omega \in \Omega$ is real.]
b) Show that $P = \sum_{g \in G} \prod_{\omega \in \Omega}(\chi(g) - \omega)$.
Deduce that $P/|G|$ is an algebraic integer.
[Hint: write P as a linear combination, with algebraic integer coefficients, of the sums $\sum_{g \in G} \chi(g)^m$, $m = 0, 1, \dots$]
c) Let N be the exponent of G, and let K_N be the field generated by the N-th roots of unity, cf. §8.7.1. Show that Ω is contained in the ring of algebraic integers of K_N and is stable under the action of its Galois group Σ_N. Deduce that P belongs to $\mathbf{Z}$, and is divisible by $|G|$.

[Note that this gives *a bound for* $|G|$ *in terms of the set* Ω, namely $|G| \leqslant P$. For an application, see exerc.6 of chap.9.]

12. (*Monomial representations and supersolvable groups.*) A linear representation V of G is called *monomial* if there exists a direct sum decomposition $V = \oplus_{i \in I} D_i$, where $\dim D_i = 1$ for every $i \in I$, which is G-stable (i.e., G permutes the D_i).
a) Let A be an abelian normal subgroup of G, and let $V = \oplus V_\chi$ be the decomposition of V according to the 1-dimensional characters χ of A. The group G permutes the V_χ. Suppose that V is irreducible; show that G permutes transitively the nonzero V_χ. Let χ be such that $V_\chi \neq 0$, and let H be the set of $g \in G$ which fix χ (i.e., $\chi(gag^{-1}) = \chi(a)$ for every $a \in A$). The group H is the stabilizer of V_χ. Suppose that the action of H on V_χ is monomial. Show that the action of G on V is monomial.
b) Suppose that G is supersolvable. Show that every representation V of G is monomial.
[Hint: reduce to the case where V is irreducible and faithful. The case where G is abelian

is clear. If G is not abelian, by part b) of exerc.13 of chap.3, there exists a normal abelian subgroup A of G which is not contained in the center of G. Apply a), and induction on $|G|$ (or on $\dim V$).]

13. a) Let m be a nonzero integer. Show that, if $\Psi^m : R(G) \to R(G)$ is injective, then m is prime to $|G|$.
[Hint: if m is not prime to $|G|$, show that there exists $g \neq 1 \in G$ which is not an m-th power; choose a nonzero virtual character χ which vanishes outside the conjugation class of g; then $\Psi^m\chi = 0$.]
b) If $G = \mathcal{A}_5$, show that Ψ^2, Ψ^3, Ψ^5 do not map $R_+(G)$ into itself.

14. Let V be a linear representation of G. Suppose that $|G|$ is odd. Show that Sym^2V has a subrepresentation isomorphic to $\wedge^2 V$.
[Hint: use Adams operation Ψ^2.]

15. (*Structure of* $\mathbf{Q} \otimes R(G)$.) Let (C_α) be a set of representatives of the conjugacy classes of the cyclic subgroups of G. For each α, let K_α be the field of rationality (cf. §8.7.3) of the generators of C_α. Show that $\mathbf{Q} \otimes R(G) \simeq \prod_\alpha K_\alpha$.
[Hint: for every α, choose a generator g_α of C_α. Show that $\chi(g_\alpha) \in K_\alpha$ for every $\chi \in R(G)$; use this to define a homomorphism $\mathbf{Q} \otimes R(G) \to \prod_\alpha K_\alpha$, and show that it is an isomorphism by using prop.8.44.]

16. (*An example of realizability.*) Let V be an irreducible representation of G, of dimension d, and let dV be the direct sum of d copies of V. Let χ be the character of V, and let k be a subfield of $\mathbf{C}$ containing the values of χ. Show that dV is realizable over k.
[Hint: use the $k[G]$-module $\varepsilon_\chi k[G]$.]

17. (*Complements to prop.8.52.*) Keep the notation of the proof of prop.8.52.
a) Show that there exists an isomorphism $E \simeq \mathbf{C}^n$ such that:
(i) E_0 is the set of (x_i) with $x_i \in \mathbf{R}$ for every i;
(ii) $\langle x, y\rangle = \sum x_i\overline{y_i}$;
(iii) $B(x, y) = \sum \lambda_i x_i y_i$, with λ_i real > 0 for every i.
b) Show that E_0 is the only $\mathbf{R}$-vector subspace of E having the following properties :
(i) $E = E_0 \oplus iE_0$.
(ii) $\langle x, y\rangle$ is real for every $x, y \in E_0$.
(iii) $B(x, x)$ is real > 0 for every $x \in E_0, x \neq 0$.

18. (*Quaternionic representations and invariant alternating forms.*)
Let $\mathbf{H}$ be the standard quaternion algebra over $\mathbf{R}$, with basis $\{1, i, j, k\}$; let $\lambda \mapsto \overline{\lambda}$ be its natural involution: $\{1, i, j, k\} \mapsto \{1, -i, -j, -k\}$.
We have $\mathbf{R} \subset \mathbf{C} \subset \mathbf{H}$. An n-dimensional left $\mathbf{H}$-vector space is the same as a $\mathbf{C}$-vector space V of dimension $2n$, together with an antilinear automorphism $j : V \to V$ such that $j^2 = -1$.
a) Let V be such an $\mathbf{H}$-vector space. A *hermitian form* on V is an $\mathbf{R}$-bilinear map $h : V \times V \to \mathbf{H}$ such that $h(\lambda x, y) = \lambda h(x, y)$ and $h(y, x) = \overline{h(x, y)}$ for every $\lambda \in \mathbf{H}$ and $x, y \in V$. The function $q_h(x) = h(x, x)$ is real valued. Show that q_h determines h via the formula:

$$4h(x, y) = \textstyle\sum_{\alpha \in Q} q_h(x + \alpha y)\alpha \quad \text{where} \quad Q = \{\pm 1, \pm i, \pm j, \pm k\}.$$

[Hint: use that $\sum_{\alpha\in Q}\alpha\lambda\alpha = -4\overline{\lambda}$ for every $\lambda \in \mathbf{H}$.]
b) A hermitian form h is called *positive definite* is $h(x,x) > 0$ for every nonzero $x \in V$. Suppose that G acts on V in an $\mathbf{H}$-linear way; this is equivalent to saying that V is a $\mathbf{C}$-representation of G such that G commutes with j. [One then says that V is a *quaternionic linear representation* of G.] Show that there exists a positive definite $\mathbf{H}$-hermitian form q on V which is invariant by G [same method as over $\mathbf{C}$]. Write $h(x,y) = A(x,y) + B(x,y)j$, where $A(x,y), B(x,y)$ belong to $\mathbf{C}$. Show that $B(x,y)$ is a nondegenerate $\mathbf{C}$-bilinear alternating form on V, which is G-invariant.
c) Conversely, let V be a $\mathbf{C}$-linear representation of G with a G-invariant nondegenerate alternating form $B(x,y)$. Show that there exists an antilinear automorphism j of V of square -1 which commutes with G; hence V is a quaternionic representation of G.
[Hint: same method as for Prop. 8.52; choose a $\mathbf{C}$-hermitian positive definite form $\langle x,y\rangle$ which is G-invariant, and write $B(x,y)$ as $\langle\phi(x),y\rangle$, where $\phi : V \to V$ is antilinear. Show that $-\phi^2$ is a positive hermitian; if b is its positive hermitian square root, take $j = \phi b^{-1}$.]

19. (*A congruence modulo p for virtual characters.*)
Let p be a prime number. Show that $(\Psi^p f - f^p)/p$ belongs to $R(G)$ for every $f \in R(G)$. [Hint: use the symmetric polynomial $\frac{1}{p}(\sum X_i^p - (\sum X_i)^p)$.]

20. (*Exterior and symmetric powers.*)
Let V be a linear representation of G, and let χ be its character. For every integer $k \geqslant 0$, let $\lambda^k\chi$ (resp. $\sigma^k\chi$) be the character of $\wedge^k V$ (resp. $\mathrm{Sym}^k V$), cf. §8.1.4. If t is an indeterminate, define the power series

$$\lambda_t(\chi) = \sum_k \lambda^k\chi\, t^k \quad \text{and} \quad \sigma_t(\chi) = \sum_k \sigma^k\chi\, t^k. \tag{8.28}$$

They belong to the ring $R(G)[[t]]$; their constant term is 1, hence they are invertible.
a) Let g be an element of G. The homomorphism $R(G) \to \mathbf{C}$ given by $f \mapsto f(g)$ transforms the series $\lambda_t(\chi)$ and $\sigma_t(\chi)$ into complex power series, which we denote by $\lambda_t(\chi)(g)$ and $\sigma_t(\chi)(g)$. Show that:

$$\lambda_t(\chi)(g) = \det(1 + g_V t) \quad \text{and} \quad \sigma_t(\chi)(g) = 1/\det(1 - g_V t), \tag{8.29}$$

where g_V is the automorphism of V defined by g.
[Hint: rewrite these formulas in terms of the eigenvalues of g_V.]
Conclude that $\lambda_t(\chi)\sigma_{-t}(\chi) = 1$.
b) Let V' be another linear representation of G and let χ' be its character. Show that

$$\lambda_t(\chi + \chi') = \lambda_t(\chi)\lambda_t(\chi') \quad \text{and} \quad \sigma_t(\chi + \chi') = \sigma_t(\chi)\sigma_t(\chi'). \tag{8.30}$$

[Hint: use the isomorphisms $\wedge(V \oplus V') \simeq \wedge V \otimes \wedge V'$ and $\mathrm{Sym}\,(V \oplus V') \simeq \mathrm{Sym}\,V \otimes \mathrm{Sym}\,V'$.]
Use these identities, together with prop.8.43, to define $\lambda_t f$ and $\sigma_t f$ for every $f \in R(G)$, and even for every class function f on G.
Show that:

$$\log \lambda_t(f) = \sum_{k=1}^{\infty} (-1)^{k-1}\Psi^k f.t^k/k \quad \text{and} \quad \log \sigma_t(f) = \sum_{k=1}^{\infty} \Psi^k f.t^k/k. \tag{8.31}$$

Deduce :

$$n\lambda^n f = \sum_{k=1}^{n}(-1)^{k-1}\Psi^k f.\lambda^{n-k} f \quad \text{and} \quad n\sigma^n f = \sum_{k=1}^{n}\Psi^k f.\sigma^{n-k} f. \tag{8.32}$$

21. (*The* 2×2-*determinants expressed in terms of traces.*) Let $A = \mathrm{M}_2(\mathbf{C})$; the determinant map $\det : A \to \mathbf{C}$ is a quadratic form on the vector space A. Let b be the associated symmetric bilinear form, characterized by $b(x,y) = \det(x+y) - \det(x) - \det(y)$, or, equivalently, by $b(x,x) = 2\det(x)$. Denote by $t(x)$ the trace $\mathrm{Tr}(x)$ of an element x of A.
a) Prove the formulas:

$$b(x,y) = t(x)t(y) - t(xy) \tag{8.33}$$

$$2\det(x) = t(x)^2 - t(x^2) \tag{8.34}$$

$$2\det(\sum x_i) = \sum_{i,j}(t(x_i)t(x_j) - t(x_ix_j)). \tag{8.35}$$

[Hint: prove first (8.34) by writing $\det(x), t(x), t(x^2)$ in terms of the two eigenvalues of x. Deduce (8.33) from (8.34) by computing the bilinear forms associated to the quadratic forms $x \mapsto t(x)^2$ and $x \mapsto t(x^2)$. Formula (8.35) follows from (8.33) by writing $2\det(\sum x_i)$ as $b(\sum x_i, \sum x_i)$.]
b) Let V be a 2-dimensional representation of a group G, and let χ be its character; for every $z \in \mathbf{C}[G]$, denote by $\det_V(z)$ the determinant of the endomorphism a_V of V defined by z. Use (8.35) to prove:

$$2\det_V(\sum X_g g) = \sum_{u,v\in G}(\chi(u)\chi(v) - \chi(uv))X_uX_v. \tag{8.36}$$

22. (*The* 3×3-*determinants expressed in terms of traces.*)
Same notation as in exerc.21, except that $A = \mathrm{M}_3(\mathbf{C})$, and that b is now the unique symmetric trilinear form such that $6\det(x) = b(x,x,x)$. Prove the formulas:

$$b(x,y,z) = t(x)t(y)t(z) - t(x)t(yz) - t(y)t(xz) - t(z)t(xy) + t(xyz) + t(yxz), \tag{8.37}$$

$$6\det(x) = t(x)^3 - 3t(x)t(x^2) + 2t(x^3), \tag{8.38}$$

$$6\det(\sum x_i) = \sum_{i,j,k} b(x_i, x_j, x_k). \tag{8.39}$$

[Hint: same method as for exerc.21, i.e., start with formula (8.38).]

b) With the same notation as in exerc.21 b), show that

$$6\det_V(\sum X_g g) = \sum_{u,v,w\in G} b_\chi(u,v,w)X_uX_vX_w, \tag{8.40}$$

where
$b_\chi(u,v,w) = \chi(u)\chi(v)\chi(w) - \chi(u)\chi(vw) - \chi(v)\chi(uw) - \chi(w)\chi(uv) + \chi(uvw) + \chi(vuw)$.

c) Show that there are similar formulas[6] in any dimension d, which express $d!\det(x)$ as a polynomial, with coefficients in $\mathbf{Z}$, in the $\mathrm{Tr}(x^n)$ with $1 \leqslant n \leqslant d$.

---

[6]It was for the purpose of finding such a formula, in the case of the regular representation, that Frobenius founded character theory, cf. [19], n°53 & n°54; for an explanation of his methods, see Curtis [17], chap.II.

23. (*Size of the coincidence locus of two characters.*) Let ϕ and ψ be two characters of G, of degrees a and b respectively; assume that $a \geqslant b$ and $a > 0$.
a) Suppose that $\phi(g) = \psi(g)$ for every $g \neq 1$. Show that there exists an integer $n \geqslant 0$ such that $\phi = \psi + n.r_G$.
[Hint: use the fact that $\langle \phi - \psi, 1 \rangle$ is an integer.]
b) Suppose that $\phi(g) - \psi(g) = -1, 0$ or 1 for every $g \in G$. Show that, either $\phi = \psi$, or there exists a homomorphism $\varepsilon : G \to \{\pm 1\}$ such that $\phi = \psi + \varepsilon$.
[Hint: write $\phi - \psi$ as a linear combination $\sum_\chi c_\chi \chi$ of irreducible characters and observe that $\sum c_\chi^2 \leqslant 1$.]
Use this result to prove that the only idempotents of the representation ring $R(G)$ are 0 and 1. [Note that such an idempotent is of the form $\phi - \psi$, with $\phi(g) - \psi(g) = 0$ or 1 for every $g \in G$.] Conclude that $R(G)$ is *indecomposable*: it is not a direct product of two nonzero rings.
c) Suppose that $\phi \neq \psi$. Let $A \subset G$ be the set of all $g \in G$ such that $\phi(g) \neq \psi(g)$. Show that $|A|/|G| \geqslant 1/a(a+b)$.
[Hint: reduce to the case where ϕ and ψ are orthogonal; use $1 \leqslant \langle \phi, \phi \rangle = \langle \phi, \phi - \psi \rangle$ and $\langle \phi, \phi - \psi \rangle \leqslant \frac{|A|}{|G|}\, a(a+b)$.]
d) By c), applied to $\psi = 0$, the set X of $g \in G$ with $\phi(g) \neq 0$ is such that $|X|/|G| \geqslant 1/a^2$. Show that there is equality when the linear representation associated to ϕ is irreducible and $\phi(g) = 0$ for every $g \notin Z(G)$. Give examples of such characters.
[Hint: take G of order p^3 and center of order p, where p is a prime, cf. exerc.5 of chap.3; show that G has $p-1$ irreducible characters of degree p, which vanish outside the center.]

24. (*Rational-valued characters.*)
a) Let χ be a virtual character of G with values in $\mathbf{Q}$. Suppose that $\sum_{c \in C} \chi(c) = 0$ for every cyclic subgroup C of G. Show that $\chi = 0$.
[Hint: reduce to the case where G is cyclic; in that case, use induction on $|G|$ and note that χ takes the same value on all the generators of G.]
b) Let V and V' be two linear representations of G. Suppose that their characters take value in $\mathbf{Z}$, and that $\dim V^C = \dim V'^C$ for every cyclic subgroup C of G. Show that $V \simeq V'$.
[Hint: apply a) to $\chi = \chi_V - \chi_{V'}$.]

25. (*Burnside's vanishing theorem.*) Let χ be a character of G, and let $B(\chi) = \prod_{g \in G} \chi(g)$.
a) Show that $B(\chi)$ is an integer.
[Hint: Show first that, if C is a cyclic subgroup of G, and C^* the set of generators of C, the product $\prod_{c \in C^*} \chi(c)$ is an integer.]
b) Suppose that χ is irreducible. Show that $B(\chi)$ is 0 if $\chi(1) > 1$. [Equivalently : every irreducible character of degree > 1 vanishes on some element of G.]
[Hint: the arithmetic mean of the $|\chi(g)|^2$ is 1; the inequality between the arithmetic and geometric means[7] implies that $B(\chi)^2 \leqslant 1$, with equality if and only if all the $|\chi(g)|^2$ are equal to 1, i.e., if $\chi(1) = 1$.]

[When one looks at the character tables of ATLAS [16], one can't help noticing their huge number of zeros, especially for the elements of large order.]

[7] If $x_1, \ldots, x_n$ are real positive numbers, then $(x_1 \cdots x_n)^{1/n} \leqslant \frac{1}{n}(x_1 + \cdots + x_n)$, with equality only if $x_1 = \cdots = x_n$.

26. (*Character table of the simple group of order* 168.) Let G be a simple group of order 168. Recall that $G \simeq \mathrm{PSL}_2(\mathbf{F}_7) \simeq \mathrm{SL}_3(\mathbf{F}_2)$, cf. §7.7 and §10.1.
a) Show that G has six conjugacy classes : 1A, 2A, 3A, 4A, 7A, 7B, of sizes 1, 21, 56, 42, 24, 24.
b) The group G acts 2-transitively on the 7 points of the projective plane over $\mathbf{F}_2$; the corresponding character splits as $1 + \chi_4$, with χ_4 irreducible of degree 6. Compute the values of χ_4.
c) Same as b) for the action of G on the 8 points of the projective line $\mathbf{P}_1(\mathbf{F}_7)$; this gives an irreducible character χ_5 of degree 7. Compute it.
d) The three remaining characters χ_2, χ_3, χ_6 have degrees a, b, c such that $a^2+b^2+c^2 = 82$. Show that two of these degrees are equal [use the fact that the class 7A is not rational, its field of rationality being $\mathbf{Q}(\sqrt{-7})$], and show that the only solution of $2a^2 + c^2 = 82$ in positive integers is $a = 3$, $c = 8$.
e) Use b), c), d) to determine the character table of G; check the result against ATLAS, [16], p.3.

27. (*Counting formulas.*) If $x \in \mathbf{C}[G]$ and $g \in G$, denote by $\delta_g(x)$ the coefficient of g in x; if $\chi \in \mathrm{Irr}(G)$, define $\chi(x)$ as $\chi(x) = \sum_g \delta_g(x)\chi(g)$.
a) If $c \in \mathbf{C}[G]^{\mathrm{cent}}$, show that $\chi(cx) = \chi(x)\chi(c)/\chi(1)$.
b) Show that $\delta_g(x) = \frac{1}{|G|}\sum_\chi \chi(1)\chi(xg^{-1})$. When x belongs to $\mathbf{C}[G]^{\mathrm{cent}}$, show that $\delta_g(x) = \frac{1}{|G|}\sum_\chi \chi(x)\chi(g^{-1})$.
c) Let $x^\sharp = \frac{1}{|G|}\sum_t txt^{-1}$. It belongs to $\mathbf{C}[G]^{\mathrm{cent}}$. If $c \in \mathbf{C}[G]^{\mathrm{cent}}$, then $(xc)^\sharp = x^\sharp c$. If $y \in \mathbf{C}[G]$, show that $\chi(x^\sharp y) = \chi(x)\chi(y)/\chi(1)$.
d) Let $u = \frac{1}{|G|^2}\sum_{x,t\in G} xtx^{-1}t^{-1}$. Show that $\chi(u) = 1/\chi(1)$.
[Hint: write u as $\frac{1}{|G|}\sum_t t^\sharp t^{-1}$, hence $\chi(u) = \frac{1}{|G|}\sum_t \chi(t^\sharp)\chi(t^{-1})/\chi(1)$ and use the fact that $\sum_t \chi(t^\sharp)\chi(t^{-1}) = \sum_t |\chi(t)|^2 = |G|$.]
Use b) to show that $\delta_g(u) = \frac{1}{|G|}\sum_\chi \chi(g^{-1})/\chi(1)$.
Show that this is equivalent to formula (8.26). [Observe that, since $\delta_g(u)$ is an integer, $\chi(g^{-1})$ can be replaced by its complex conjugate $\chi(g)$.]
e) Let $z_1, \ldots, z_k$ be elements of G. Let $M(z_1, \ldots, z_k)$ be the number of k-tuples $(x_1, \ldots, x_k)$ such that

$$x_1z_1x_1^{-1}.x_2z_2x_2^{-1}\cdots x_kz_kx_k^{-1} = 1.$$

Show that

$$M(z_1, \ldots, z_k) = |G|^{k-1} \sum_{\chi\in\mathrm{Irr}(G)} \frac{\chi(z_1)\cdots\chi(z_k)}{\chi(1)^{k-2}}. \tag{8.41}$$

[Hint: put $v = \frac{1}{|G|^k}\sum_{x_1,\ldots,x_k} x_1z_1x_1^{-1}\cdots x_kz_kx_k^{-1} = z_1^\sharp\cdots z_k^\sharp$. Use c) to show that $\chi(v) = \chi(z_1)\cdots\chi(z_k)/\chi(1)^{k-1}$, and apply d).]
Show that (8.41) is equivalent to (8.27).

28. (*Characters of quotient groups.*) Let N be a normal subgroup of G, and let $\Gamma = G/N$. If f is a central function on G, let f_Γ be the function on Γ defined by $\gamma \mapsto \frac{1}{|N|}\sum_{g\mapsto\gamma} f(g)$.
a) Suppose that V is a linear representation of G with character f. The group Γ acts on V^N. Show that the character of that representation is f_Γ.
b) Show that $f \in R_+(G) \Longleftrightarrow f_\Gamma \in R_+(\Gamma)$ and $f \in R(G) \Longleftrightarrow f_\Gamma \in R(\Gamma)$.

c) Show that a) and b) remain true for G not necessarily finite, and for any ground field k, provided that N is finite of order invertible in k.

29. (*Induced representations.*) Here G is not necessarily finite, and the ground field is an arbitrary field k.
Let H be a subgroup of G of finite index, let V be a k-linear representation of G, and let W be a subspace of V which is stable under the action of H. If $x \in G/H$, the space gW, where g is a representative of x in G, only depends on x; we denote it by xW.

a) The G-representation V is said to be *induced* by the H-representation W if we have $V = \oplus_{x \in G/H} xW$, i.e., if V is the direct sum of the xW.
Suppose this is the case. Let E be a representation of G. Show that every H-homomorphism of W into E extends uniquely to a G-homomorphism $V \to E$. This gives an isomorphism $\mathrm{Hom}_H(W, E) \simeq \mathrm{Hom}_G(V, E)$.

b) Let W be a representation of H. Show that there exists a representation V of G which is induced by W.
[Hint: give a direct construction; or define V as $V = k[G] \otimes_{k[H]} W$; or define V as the vector space of all maps $f : G \to W$ such that $f(hx) = hf(x)$ for every $x \in G$ and $h \in H$, the action of G on V being $(gf)(x) = f(xg)$.]
That representation is unique, up to isomorphism; we denote it by $\mathrm{Ind}_H^G W$.

c) If W is the trivial 1-dimensional representation of H, show that $\mathrm{Ind}_H^G W$ is isomorphic to the permutation representation $k^{G/H}$, cf. §8.1.5.

d) Show that a representation of G is monomial (cf. exerc.12) if and only if it is a direct sum of representations of the form $\mathrm{Ind}_{H_i}^G W_i$ where the H_i are subgroups of finite index of G, and the W_i are 1-dimensional representations of the H_i.

30. (*Induced characters.*) The notation is the same as in exerc.29 above.
a) Let f be a class function on H with values in an abelian group A. Define a function $\mathrm{Ind}_H^G f$ on G by the formula

$$\mathrm{Ind}_H^G f(g) = \sum_{x \in G/H \text{ and } x^{-1}gx \in H} f(x^{-1}gx). \tag{8.42}$$

[Note that $f(x^{-1}gx)$ depends only on the coset xH because f is a class function on H.]
Show that $\mathrm{Ind}_H^G f$ is a class function on G. If F is a class function on G, let F_H denotes its restriction to H. Show that $\mathrm{Ind}_H^G(fF_H) = \mathrm{Ind}_H^G(f)F$. If G is finite and $k = \mathbf{C}$, show that

$$\langle f, F_H \rangle_H = \langle \mathrm{Ind}_H^G f, F \rangle_G. \tag{8.43}$$

b) Let W be a linear representation of H, with character χ_W, and let $\mathrm{Ind}_H^G W$ be the linear representation of G induced by W. Show that the character of $\mathrm{Ind}_H^G W$ is $\mathrm{Ind}_H^G \chi_W$.
[Hint: use exerc.32 a).]
If G is finite and $k = \mathbf{C}$, show that Ind_H^G defines a map $R(H) \to R(G)$, which is additive, and sends $R_+(H)$ to $R_+(G)$.

31. (*Characteristic polynomials for direct sums.*)
Let k be a field and V a k-vector space of finite dimension v. If $g \in \mathrm{End}(V)$, denote by $P(V, g; t)$ the characteristic polynomial of g, i.e.,$\det_V(t - g)$.
a) Let $V = \oplus_{x \in X} W_x$ be a direct sum decomposition of V, indexed by a finite set X. Let

γ be a permutation of X, and suppose that $gW_x = W_{\gamma x}$ for every $x \in X$.
Let O_α be the orbits in X of the cyclic group $C_\gamma = \langle \gamma \rangle$ generated by γ; for every α, let x_α be a point of O_α; put $n_\alpha = |O_\alpha|$. The endomorphism g^{n_α} stabilizes W_{x_α}.
Show that

$$P(V, g; t) = \prod_\alpha P(W_{x_\alpha}, g^{n_\alpha}; t^{n_\alpha}). \tag{8.44}$$

[Hint: it is enough to prove (8.44) when C_γ acts transitively on X, in which case all the W_x have the same dimension w; do first the case where $w = 1$; then use induction on w, assuming (as one may) that k is algebraically closed.]
b) Use (8.44) to prove:

$$\mathrm{Tr}_V(g) = \sum_{\alpha, n_\alpha = 1} \mathrm{Tr}_{W_{x_\alpha}}(g), \tag{8.45}$$

and

$$\mathrm{det}_V(g) = \prod_\alpha (-1)^{w_\alpha(n_\alpha - 1)} \mathrm{det}_{W_{x_\alpha}}(g^{n_\alpha}), \tag{8.46}$$

where $w_\alpha = \dim W_{x_\alpha}$.
[Hint: for (8.46), note that the constant term of the polynomial $P(V, g; t)$ is $(-1)^v \mathrm{det}_V(g)$, while that of $P(W_{x_\alpha}, g^{n_\alpha}; t^{n_\alpha})$ is $(-1)^{w_\alpha} \mathrm{det}_{W_{x_\alpha}}(g^{n_\alpha})$.]

32. (*Traces and determinants for induced representations.*)
Let $G, H, V, W, X = G/H$ be as in exerc.29 and let g be an element of G. Let γ be the permutation of X defined by g; as in exerc.31, let O_α be the orbits of $C_\gamma = \langle \gamma \rangle$ in X, let x_α be a point of O_α, and let $n_\alpha = |O_\alpha|$.
a) Use (8.45) to prove:
$$\chi_V(g) = \sum_{\alpha, n_\alpha = 1} \chi_W(x_\alpha^{-1} g x_\alpha). \tag{8.47}$$
[Hint: show first that $\mathrm{Tr}_{W_{x_\alpha}}(g) = \chi_W(x_\alpha^{-1} g x_\alpha)$.]
b) The determinant of $G \to \mathrm{GL}_V$ may be viewed as a homomorphism $\mathrm{det}_V : G^{\mathrm{ab}} \to k^\times$. Define similarly $\mathrm{det}_W : H^{\mathrm{ab}} \to k^\times$. Use (8.46) to prove:
$$\mathrm{det}_V(g) = \epsilon_H(g)^{\dim W} \mathrm{det}_W(\mathrm{Ver}_H^G(g)), \tag{8.48}$$
where $\epsilon_H(g)$ is the signature of the permutation γ, and $\mathrm{Ver}_H^G : G^{\mathrm{ab}} \to H^{\mathrm{ab}}$ is the transfer map of chap.7.
[Hint: use th.7.5.]

33. (*Tensor induction and transfer.*)
Let G, H, V, W, X be as in exerc.29. Let $E = \otimes_{x \in X}\, xW$ be the tensor product of the xW. There is a natural action of G on E; in that action, a tensor product $\otimes_{x \in X} w_x$, where w_x belongs to xW, is mapped by $g \in G$ to $\otimes_{x \in X}\, g w_{g^{-1}x}$. The G-space so obtained is called the *tensor induction* of W.
Suppose that $\dim W = 1$, hence $\dim E = 1$. Let $\chi_W : H^{\mathrm{ab}} \to k^\times$ be the corresponding character; define similarly $\chi_E : G^{\mathrm{ab}} \to k^\times$. Show that:
$$\chi_E = \chi_W \circ \mathrm{Ver}_H^G. \tag{8.49}$$

34. (*Using induced characters to simplify the proof of Frobenius's theorem 6.7.*)
With the notation of §8.10, show that, if $f(1) = 0$, then $\tilde{f} = \mathrm{Ind}_H^G f$, in which case formula (8.23) : $\langle \tilde{f}, \theta_H \rangle_G = \langle f, \theta_H \rangle_H$ follows from (8.43). This gives a direct proof that $f \in R(H) \Longrightarrow \tilde{f} \in R(G)$.

Chapter 9

Finite subgroups of GL_n

This chapter gives two boundedness theorems on a finite subgroup G of $\mathrm{GL}_n(k)$:

• the first one (Minkowski [68]) assumes that $k = \mathbf{Q}$ and gives a multiplicative bound for $|G|$;

• the second one (Jordan [62]) assumes that $k = \mathbf{C}$, and shows the existence of an abelian normal subgroup of G whose index is bounded by a constant depending only on n.

9.1 Minkowski's theorem on the finite subgroups of $\mathrm{GL}_n(\mathbf{Q})$

9.1.1. Statement of the theorem.

Let G be a finite subgroup of $\mathrm{GL}_n(\mathbf{Q})$. In [68], Minkowski showed that **the order of G is bounded by a function of n.** More precisely, he defined for every $n \geqslant 0$ an integer $M(n) > 0$ (see below) and proved :

Theorem 9.1. (1) *The order of a finite subgroup of* $\mathrm{GL}_n(\mathbf{Q})$ *divides* $M(n)$.
(2) $M(n)$ *is the smallest integer having property* (1).

The definition of $M(n)$ is as follows: for every prime number ℓ, put:

$$M(n,\ell) = [\frac{n}{\ell-1}] + [\frac{n}{\ell(\ell-1)}] + [\frac{n}{\ell^2(\ell-1)}] + \cdots, \tag{9.1}$$

where the brackets [ ] mean "integral part", and define $M(n)$ as :

$$M(n) = \prod_{\ell} \ell^{M(n,\ell)}. \tag{9.2}$$

Examples.
For $n = 2$, we have $M(2,2) = 2+1 = 3, M(2,3) = 1, M(2,\ell) = 0$ for $\ell > 3$, so that

$M(2) = 2^3.3 = 24$. The orders of the finite subgroups of $\mathrm{GL}_2(\mathbf{Q})$ are $1, 2, 3, 4, 6, 8, 12$, so that their l.c.m. is indeed 24.
Other examples are:

$$M(0) = 1,\ M(4) = 5760,\ M(6) = 2903040,\ M(8) = 1393459200.$$

[Note that $M(2k+1) = 2M(2k)$, hence it is enough to give the value of $M(n)$ when n is even.]

Minkowski's proof of part (1) consisted in proving :

(a) If G is a finite subgroup of $\mathrm{GL}_n(\mathbf{Q})$, then $|G|$ divides $|\mathrm{GL}_n(\mathbf{F}_p)|$ for every prime $p > 2$.
(b) If $\ell > 2$, there are infinitely many primes p such that the ℓ-component of $|\mathrm{GL}_n(\mathbf{F}_p)|$ is $\ell^{M(n,\ell)}$.
(c) Similar statement for $\ell = 2$, with GL_n replaced by an orthogonal group O_n.

We shall follow his method, with a few minor changes.

9.1.2. First reductions.

Assertion (1) is essentially a question about ℓ-groups. More precisely:

Lemma 9.2. *Assertion* (1) *is equivalent to* :
(1′) *If ℓ is a prime number, and A is a finite ℓ-subgroup of* $\mathrm{GL}_n(\mathbf{Q})$, *then* $|A| \leqslant \ell^{M(n,\ell)}$.

Proof. (1) $\Longrightarrow$ (1′) is clear. The converse follows from Sylow's theorem.

In what follows, the prime number ℓ is fixed, and so is the ℓ-group $A \subset \mathrm{GL}_n(\mathbf{Q})$.

Let us choose an integer $q > 2$ such that A *is contained in* $\mathrm{GL}_n(\mathbf{Z}[1/q])$. This is possible: take for q the product of all the denominators of the coefficients of the matrices belonging to A.
If p is a prime number which does not divides q, then q is invertible in $\mathbf{F}_p$ and there is a unique ring homomorphism $\mathbf{Z}[1/q] \to \mathbf{F}_p$, hence also a homomorphism

$$\mathrm{GL}_n(\mathbf{Z}[1/q]) \ \to\ \mathrm{GL}_n(\mathbf{F}_p).$$

Lemma 9.3. *If p is large enough, the homomorphism*

$$A \ \to\ \mathrm{GL}_n(\mathbf{Z}[1/q]) \ \to\ \mathrm{GL}_n(\mathbf{F}_p)$$

is injective.

Proof. For every $a \in A - \{1\}$, choose a coefficient x_a of the matrix $q(a-1)$ which is a nonzero integer. If p does not divide $q\prod_{a\neq 1} x_a$, the kernel of $A \ \to\ \mathrm{GL}_n(\mathbf{F}_p)$ is trivial.

Lemma 9.4. *If p is large enough, the order of A divides* $r_n(p) = \prod_{i=1}^{n}(p^i - 1)$.

Proof. By lemma 9.3, A is isomorphic to a subgroup of $\mathrm{GL}_n(\mathbf{F}_p)$. Hence its order divides the order of $\mathrm{GL}_n(\mathbf{F}_p)$, which is equal to $p^{n(n-1)/2}r_n(p)$. Since A is an ℓ-group and $\ell \neq p$, this implies that $|A|$ divides $r_n(p)$.

9.1.3. ℓ-adic estimates.

We keep the notation of §9.1.2. Recall (cf. §4.8) that, if x in a nonzero integer, $v_\ell(x)$ is the *ℓ-adic valuation of* x, i.e., the largest integer m such that ℓ^m divides x.

Lemma 9.5. *Let m be an integer > 0. Then :*

$$v_\ell(m!) = [\frac{m}{\ell}] + [\frac{m}{\ell^2}] + [\frac{m}{\ell^3}] + \cdots \tag{9.3}$$

Proof. For every j, let a_j be the number of $z \in [1, m]$ such that $v_\ell(z) = j$. We have $v_\ell(m!) = \sum_{z=1}^m v_\ell(z) = \sum_j j a_j$, and $a_j = b_j - b_{j+1}$ where $b_j = [m/\ell^j]$. Hence:

$$\begin{aligned} v_\ell(m!) &= a_1 + 2a_2 + 3a_3 + \cdots \\ &= (b_1 - b_2) + 2(b_2 - b_3) + 3(b_3 - b_4) + \cdots \\ &= b_1 + b_2 + b_3 + \cdots \end{aligned}$$

Lemma 9.6. *Let (x, a, b) be integers such that $a, b \geqslant 1$.Then $[[x/a]/b] = [x/ab]$.*

Proof. We have $x = ay + \epsilon$ with $y = [x/a]$ and $0 \leqslant \epsilon \leqslant a - 1$. If $z = [y/b]$, we have $y = bz + \eta$ with $0 \leqslant \eta \leqslant b-1$. Hence $x = abz + a\eta + \epsilon \leqslant abz + a(b-1) + a - 1 = abz + ab - 1$; this shows that $[x/ab] = z$.

We now assume that $\ell \neq 2$. This implies that *the multiplicative group $(\mathbf{Z}/\ell^2\mathbf{Z})^\times$ is cyclic of order $\ell(\ell-1)$*; indeed, that group is an extension of $(\mathbf{Z}/\ell\mathbf{Z})^\times$, which is cyclic of order $\ell - 1$, by a cyclic group of order ℓ; since ℓ and $\ell - 1$ are relatively prime, the extension splits.

Lemma 9.7. *Let $x \in \mathbf{Z}$ be such that the class of x mod ℓ^2 generates $(\mathbf{Z}/\ell^2\mathbf{Z})^\times$. Let k be an integer $\geqslant 1$. Then :*

$$v_\ell(x^k - 1) = \begin{cases} 0 & \textit{if } k \textit{ is not divisible by } \ell - 1, \\ v_\ell(k) + 1 & \textit{if } k \textit{ is divisible by } \ell - 1. \end{cases}$$

Proof. If $\ell - 1$ does not divide k, then $x^k \not\equiv 1 \pmod{\ell}$ and $v_\ell(x^k - 1) = 0$.
If $k = (\ell - 1)m$ with $m \geqslant 1$, we have $x^k = y^m$, where $y = x^{\ell-1}$. The hypothesis made on x implies that $y = 1 + \ell z$, with $\ell \nmid z$. Let us write m as $m = r\ell^a$, with $a = v_\ell(m) = v_\ell(k)$. We then have:

$$y^m = (y^{\ell^a})^r = (1 + \ell^{a+1}z + \cdots)^r = 1 + \ell^{a+1}zr + \cdots,$$

where the unwritten terms are divisible by ℓ^{a+2}.
This shows that $v_\ell(y^m - 1) = a + 1$, i.e., $v_\ell(x^k - 1) = v_l(k) + 1$.

Lemma 9.8. *Let $x \in \mathbf{Z}$ be as in lemma 9.7. Then*

$$v_\ell(\prod_{i=1}^n (x^i - 1)) = M(n, \ell). \tag{9.4}$$

Proof. Let $N = \prod_{i=1}^n (x^i - 1)$. We have $v_\ell(N) = \sum_{i=1}^n v_\ell(x^i - 1)$. By lemma 9.7, $v_\ell(x^i - 1) = 0$ if i is not divisible by $\ell - 1$; the other indices i can be written as $i = (\ell - 1)y$, with $1 \leqslant y \leqslant m = [n/(\ell-1)]$. We thus have $v_\ell(N) = \sum_{y=1}^m v_\ell(x^{(\ell-1)y} - 1)$; by lemma 9.7, this gives:

$$v_\ell(N) = \sum_{y=1}^{m} (1 + v_\ell((\ell-1)y)) = \sum_{y=1}^{m} (1 + v_\ell(y)) = m + v_\ell(m!) = m + [m/\ell] + [m/\ell^2] + \cdots,$$

cf. lemma 9.5. By lemma 9.6, we have $[m/\ell^\alpha] = [n/(\ell-1)\ell^\alpha]$. Hence:

$$v_\ell(N) = \sum_{\alpha \geqslant 0} [n/(\ell-1)\ell^\alpha] = M(n,\ell).$$

9.1.4. Proof of part (1) of theorem 9.1.

Instead of (1), we prove (1′) for every prime ℓ, cf. lemma 9.2.

(i) *The case* $\ell > 2$.

By *Dirichlet's theorem on arithmetic progressions* (see e.g. [36], chap. 6), we can find an arbitrary large prime p such that its class mod ℓ^2 generates $(\mathbf{Z}/\ell^2\mathbf{Z})^\times$. By lemma 9.8, we have $v_\ell(r_n(p)) = M(n,\ell)$. By lemma 9.4, we have $v_\ell(|A|) \leqslant v_\ell(r_n(p))$, hence $|A| \leqslant \ell^{M(n,\ell)}$.

(ii) *The case* $\ell = 2$.

Here, embeddings in $\mathrm{GL}_n(\mathbf{F}_p)$ do not give enough information. One needs to observe that the group G preserves a nondegenerate quadratic form with coefficients in $\mathbf{Q}$. By a reduction process similar to that of lemma 9.3, this implies that the group G (or its 2-Sylow subgroup A) embeds, for large p, in an orthogonal group $\mathrm{O}_n(\mathbf{F}_p)$. One then replaces $r_n(p)$ by the index $o_n(p)$ of a p-Sylow subgroup of $\mathrm{O}_n(\mathbf{F}_p)$.
Assume first that n is odd, and let $r = [n/2]$. Choose $p \equiv \pm 3 \pmod 8$. The order of $\mathrm{O}_n(\mathbf{F}_p)$ is known to be $2p^{r^2} \prod_{i=1}^r (p^{2i} - 1)$. Hence $o_n(p) = 2\prod_{i=1}^r (p^{2i} - 1)$, and its 2-adic valuation is :

$$1 + \sum_{i=1}^{r} (3 + v_2(i)) = 1 + 3r + v_2(r!) = n + r + [r/2] + [r/4] + \cdots = M(n,2);$$

this implies $v_2(|A|) \leqslant v_2(o_n(p)) = M(n,2)$, as desired.
The case where n is even follows from the case where n is odd, cf. exerc.4.

There is a different proof, based on character theory, which applies equally well to (i) and (ii), see exerc.6. That proof is due to I. Schur. It gives a slightly stronger result than Minkowski's proof: it shows that, if G is a finite subgroup of $\mathrm{GL}_n(\mathbf{C})$ *such that* $\mathrm{Tr}(g) \in \mathbf{Q}$ *for every* $g \in G$, then $|G|$ divides $M(n)$.

[Note that this condition is less restrictive than $G \subset \mathrm{GL}_n(\mathbf{Q})$, as the case of the quaternion subgroup of $\mathrm{GL}_2(\mathbf{C})$ shows.]

9.1.5. Proof of part (2) of theorem 9.1.

Let ℓ be a prime number. We have to construct a subgroup G of $\mathrm{GL}_n(\mathbf{Q})$ such that $v_\ell(|G|) = M(n, \ell)$.

Let $m = [n/(\ell - 1)]$. We have $M(n, \ell) = M(m(\ell - 1), \ell)$. Hence we may replace n by $m(\ell - 1)$. The cyclic group C_ℓ of order ℓ has a faithful representation in $\mathrm{GL}(V_1)$, where V_1 is a $\mathbf{Q}$-vector space of dimension $\ell - 1$. Let $V = V_1 \oplus \cdots \oplus V_m$ be the direct sum of m copies of V_1. Let C be the product of m copies of C_ℓ; it acts on V (diagonal action). The symmetric group $\mathcal{S}_m$ also acts on V, by permuting the factors. We thus get an action on V of the semidirect product G of $\mathcal{S}_m$ and C. This gives an embedding of G in $\mathrm{GL}(V) \simeq \mathrm{GL}_n(\mathbf{Q})$. We have

$$v_\ell(|G|) = v_\ell(C) + v_\ell(\mathcal{S}_n) = m + v_\ell(m!) = m + [m/\ell] + [m/\ell^2] + \cdots ,$$

which is equal to $M(n, \ell)$, cf. proof of lemma 9.8.

9.1.6. Complements.

a) The theorem implies that $|G| \leqslant M(n)$, but this bound is usually not optimal, as the case $n = 2$ already shows.

b) There is a Sylow-like theorem for finite ℓ-subgroups of $\mathrm{GL}_n(\mathbf{Q})$, cf. [36], §1.5 : if A is an ℓ-subgroup of order $\ell^{M(n,\ell)}$, then every ℓ-subgroup of $\mathrm{GL}_n(\mathbf{Q})$ is conjugate to a subgroup of A. In particular, the maximal finite ℓ-subgroups are conjugate.

c) Minkowski's idea of reducing mod p can be applied to other algebraic groups than GL_n and to other fields than $\mathbf{Q}$, cf. [36]. The main difference is that Dirichlet's theorem on arithmetic progressions has to be replaced by a suitable generalization of Chebotarev's density theorem, cf. [36], §6.4.

As an example, let G be a finite subgroup of $E(k)$, where E is an algebraic linear group of type E_8 over a field k of characteristic 0; suppose that k does not contain any abelian nontrivial extension of $\mathbf{Q}$. Then $|G|$ divides $2^{30}.3^{13}.5^5.7^4.11^2.13^2.19.31$, cf. [36], §6.3.2; here also, the bound is optimal ([36], §7, cor. to th.11).

9.2 Jordan's theorem on the finite subgroups of $\mathrm{GL}_n(\mathbf{C})$

9.2.1. Statement of the theorem.

The order of a finite subgroup of $\mathrm{GL}_n(\mathbf{C})$ cannot be bounded by a function of n, as the case $n = 1$ already shows. But this example, and other less obvious ones, suggests that this is due to the existence of large abelian subgroups. The precise formulation is due to Jordan [62] (for a recent exposition of his proof, see Breuillard [45]):

Theorem 9.9. *For every $n \geqslant 1$, there exists a real number $f(n)$ such that every finite subgroup of $\mathrm{GL}_n(\mathbf{C})$ contains an abelian normal subgroup of index $\leqslant f(n)$.*

For instance, if $n = 1$ (resp. $n = 2$) one may take $f(n) = 1$ (resp. $f(n) = 60$).

We shall prove th.9.9 in §9.2.6 by using a method of Frobenius ([19], n°87) which gives an explicit value for $f(n)$, namely :

$$f(n) = (\sqrt{8n}+1)^{2n^2} - (\sqrt{8n}-1)^{2n^2}. \tag{9.5}$$

There are three steps in the proof:

(i) Replace $\mathrm{GL}_n(\mathbf{C})$ by the unitary group $\mathbf{U}_n(\mathbf{C})$; this is possible, thanks to prop.8.8.

(ii) Construct an open neighborhood U of 1 in $\mathbf{U}_n(\mathbf{C})$ such that:

- it is stable under the inner automorphisms of $\mathbf{U}_n(\mathbf{C})$.
- every finite subgroup A of $\mathbf{U}_n(\mathbf{C})$ generated by $A \cap U$ is abelian.

This will be done in §9.2.4, the set U being made up of the unitary matrices u with $N(1-u) < 1/2$, where N is the square of the Hilbert-Schmidt norm, cf. §9.2.3.

(iii) If $G \subset \mathbf{U}_n(\mathbf{C})$ is finite, and if A is the abelian normal subgroup of G generated by $G \cap U$, show that $(G : A)$ is bounded by $f(n)$.

This will done by a packing argument.

9.2.2. Finite dimensional hermitian spaces, and normal operators.

In this section, and in the next ones, V is an n-dimensional $\mathbf{C}$-vector space, endowed with a positive definite hermitian form $h(x,y)$, cf. §8.2.2. We write this form as $\langle x,y\rangle$, and we put $|x| = \langle x,x\rangle^{1/2}$; hence $|x-y|$ is the usual euclidean distance on V.

An element x of V such that $|x| = 1$ is called a **unit vector**. A basis $(e_1,\ldots,e_n)$ of V is called an **orthonormal basis** of V if the e_i are unit vectors, and they are orthogonal to each other. This is equivalent to $\langle e_i, e_j\rangle = \delta_i^j$, where δ_i^j is the *Kronecker symbol*, i.e., 1 if $i = j$, and 0 if $i \neq j$. The choice of such a basis identifies V to $\mathbf{C}^n$, with its standard hermitian form $\langle x,y\rangle = \sum x_i\overline{y_i}$.

Let M be the algebra $\mathrm{End}(V) \simeq \mathrm{M}_n(\mathbf{C})$. If $a \in M$, its **adjoint** a^* is the unique element of M such that:

$$\langle ax,y\rangle = \langle x,a^*y\rangle \quad \text{for all } x,y \in V. \tag{9.6}$$

We have $(a^*)^* = a$, and $(ab)^* = b^*a^*$.
If (a_{ij}) is the matrix of a with respect to an orthonormal basis, the matrix of a^* is $(\overline{a_{ji}})$, i.e., it is the complex conjugate of the transpose of (a_{ij}).

An element $a \in M$ is called **normal** if $aa^* = a^*a$. The two main examples are:
1) The **hermitian** case : $a^* = a$; it is equivalent to $\langle ax,y\rangle$ being a hermitian form; it is also equivalent to $\langle ax,x\rangle \in \mathbf{R}$ for every $x \in V$; when $\langle ax,x\rangle \geqslant 0$ for every $x \in V$, then a is called a **positive hermitian**.

2) The **unitary** case: $aa^* = 1$, i.e., $\langle ax, ay\rangle = \langle x, y\rangle$ for every $x, y \in V$, i.e., a is an automorphism of the pair (V, h). The unitary elements make up a subgroup $\mathbf{U}_V$ of $M^\times = \mathrm{GL}(V)$. When $V = \mathbf{C}^n$ with its standard hermitian form, $\mathbf{U}_V$ is the group $\mathbf{U}_n(\mathbf{C})$ of $n \times n$ unitary matrices.

Proposition 9.10. *Let $a \in M$ be normal. Then :*
(1) If $x \in V$ is such that $ax = \lambda x$, $\lambda \in \mathbf{C}$, then $a^*x = \overline{\lambda}x$; if $y \in V$ is such that $\langle x, y\rangle = 0$, then $\langle x, ay\rangle = 0$ and $\langle x, a^*y\rangle = 0$.
(2) There exists an orthonormal basis of V made up of eigenvectors of a.

Proof of (1). After replacing a by $a - \lambda$ and a^* by $a^* - \overline{\lambda}$, we may assume that $\lambda = 0$. We then have $\langle a^*x, a^*x\rangle = \langle x, aa^*x\rangle = \langle x, a^*ax\rangle = 0$, hence $a^*x = 0$. If $\langle x, y\rangle = 0$, then $\langle x, ay\rangle = \langle a^*x, y\rangle = 0$, and the same argument shows that $\langle x, a^*y\rangle = 0$.
Proof of (2). Use induction on n. Choose a unit eigenvector e_1 of a. Let H be the hyperplane orthogonal to e_1. By (1), H is stable under the action of a; the induction hypothesis implies that there exists an orthonormal basis $(e_2, \ldots, e_n)$ of H made up of eigenvectors of a; we thus obtain an orthonormal basis $(e_1, \ldots, e_n)$ of V such that each e_i is an eigenvector of a.

Remark. If the orthonormal basis is chosen as in (2), the matrix of a is a diagonal matrix whose diagonal entries are the eigenvalues $(\lambda_1, \ldots, \lambda_n)$ of a; the matrix of a^* is diagonal with diagonal entries $\overline{\lambda_1}, \ldots, \overline{\lambda_n}$. This shows that *a normal endomorphism is hermitian* (resp. positive hermitian, resp. unitary) *if and only if its eigenvalues are real* (resp. are real $\geqslant 0$, resp. have absolute value 1).

Corollary 9.11. *Let $a \in M$ be positive hermitian and let m be an integer $\geqslant 1$. There exists a unique positive hermitian b such that $a = b^m$.*

Proof. Let L be the set of eigenvalues of a; since a is positive hermitian, the elements of L are real $\geqslant 0$, and E is the orthogonal direct sum $E = \oplus_{\lambda \in L} E_\lambda$ of the corresponding eigenspaces E_λ, cf. prop.9.10. The automorphism b of E such that $bx = \lambda^{1/m}x$ if $x \in E_\lambda$ is positive hermitian, and such that $a = b^m$. If b' is another such automorphism, its set M of eigenvalues is made up of the positive m-th roots of the elements of L, and we have a corresponding eigenspace decomposition $E = \oplus_{\mu \in M} E(\mu)$. Since $a = b'^m$, the automorphism a is $x \mapsto \mu^m x$ on $E(\mu)$; hence $E(\mu) = E_\lambda$ with $\lambda = \mu^m$ and this shows that $b' = b$.

9.2.3. The norm of an endomorphism.

Let $a \in M$. The **norm** $N(a)$ of a is defined by:

$$N(a) = \mathrm{Tr}(aa^*) = \mathrm{Tr}(a^*a). \tag{9.7}$$

[In Hilbert space theory, $N(a)^{1/2}$ is called the *Hilbert-Schmidt norm* of a.]

If (a_{ij}) is the matrix of a with respect to an orthonormal basis (e_i), we have:

$$N(a) = \sum_{i,j} |a_{ij}|^2 = \sum_i |ae_i|^2. \tag{9.8}$$

The following proposition gives the properties of the norm which will be needed in the next section:

Proposition 9.12. (1) $N(1) = n$.

(2) *If u is unitary, then $N(ua) = N(au) = N(a)$ for every $a \in M$.*

(3) *If a is normal, with eigenvalues λ_i, then $N(a) = \sum |\lambda_i|^2$.*

(4) *If a is normal, then $N(ab - ba) \leqslant 2N(a)N(b)$ for every $b \in M$.*

(5) *If u, v are unitary, then $N(1 - uvu^{-1}v^{-1}) \leqslant 2N(1-u)N(1-v)$.*

(6) *If u, v are unitary, define inductively $v_0 = v, v_1, v_2, \ldots$ by $v_m = uv_{m-1}u^{-1}v_{m-1}^{-1}$. Then $N(1 - v_m) \leqslant 2^m N(1-u)^m N(1-v)$.*

Proof of (1). It follows from $\mathrm{Tr}(1) = n$.

Proof of (2). If u is unitary, then $au(au)^* = auu^{-1}a^* = aa^*$, hence $N(au) = N(u)$. Similarly, $ua(ua)^* = a^*a$, hence $N(ua) = N(a)$.

Proof of (3). If a is normal, prop.9.10 shows the existence of an orthonormal basis (e_i) with respect to which a is a diagonal matrix with $(\lambda_1, \ldots, \lambda_n)$ on the diagonal, and similarly for a^*, with $\overline{\lambda_1}, \ldots, \overline{\lambda_n}$ on the diagonal. The trace of aa^* is thus $\sum |\lambda_i|^2$.

Proof of (4). Choose an orthonormal basis as in (3). If (b_{ij}) is the matrix of b, the matrix of $ab - ba$ is $((\lambda_i - \lambda_j)b_{ij})$. Hence

$$N(ab - ba) = \sum_{i,j} |\lambda_i - \lambda_j|^2 |b_{ij}|^2 \leqslant L.N(b), \quad \text{where } L = \sup_{i<j} |\lambda_i - \lambda_j|^2.$$

Since $|\lambda_i - \lambda_j|^2 + |\lambda_i + \lambda_j|^2 = 2(|\lambda_i|^2 + |\lambda_j|^2)$, we have

$$L \leqslant 2 \sup_{i<j}(|\lambda_i|^2 + |\lambda_j|^2) \leqslant 2N(a),$$

cf. (3). Hence $N(ab - ba) \leqslant 2N(a)N(b)$.

Proof of (5). By (2), applied to u and v, we have :

$$N(1 - uvu^{-1}v^{-1}) = N(vu - uv) = N(v'u' - u'v'),$$

where $u' = 1-u$ and $v' = 1-v$. By (4), this gives $N(1-uvu^{-1}v^{-1}) \leqslant 2N(1-u)N(1-v)$.

Proof of (6). It follows from (5), by induction on m.

9.2.4. Construction of abelian subgroups.

Proposition 9.13. *Let $u, v \in M$ be unitary, and let $c = uvu^{-1}v^{-1}$. Suppose that u and c commute and that $N(1-v) < 2$. Then u and v commute.*
[The condition $N(1-v) < 2$ can be weakened to $N(1-v) < 4$, which is best possible, cf. exerc.7.]

Proof. Let $u' = u^{-1}c = vuv^{-1}$. Since u and c commute, the same is true for u and u'. By applying prop.9.10 to u, and then to u', we may find an orthonormal basis $(e_1, \ldots, e_n)$ made up of eigenvectors of both u and u'. Let $(\lambda_1, \ldots, \lambda_n, \lambda'_1, \ldots, \lambda'_n)$ be the corresponding eigenvalues. If $\lambda_i = \lambda'_i$ for every i, then $u' = u$, which means that u and v commute. If not, let i be such that $\lambda_i \neq \lambda'_i$. Since e_i is an eigenvector of u with eigenvalue λ_i, then ve_i is an eigenvector of $u' = vuv^{-1}$ with eigenvalue λ_i. Hence e_i and ve_i are eigenvectors of u' corresponding to distinct eigenvalues. This implies that they are orthogonal. Hence $|(1-v)e_i|^2 = |e_i - ve_i|^2 = |e_i|^2 + |ve_i|^2 = 2$. By formula (9.8), this implies $N(1-v) \geqslant 2$, contrary to the hypothesis made on v. Hence this case is impossible, and we have $uv = vu$.

Proposition 9.14. *Let u and v be elements of a finite subgroup of the unitary group $\mathbf{U}_V$. If $N(1-u) < 1/2$ and $N(1-v) < 2$, then u and v commute.*
[Here also, $N(1-v) < 2$ can be replaced by $N(1-v) < 4$.]

Proof. Define $v_0, v_1, \ldots$ by induction, with $v_0 = v$ and $v_m = uv_{m-1}u^{-1}v_{m-1}^{-1}$ for $m \geqslant 1$. By part (6) of prop.9.12, we have

$$N(1-v_m) \leqslant 2^m N(1-u)^m N(1-v) < 2. \tag{9.9}$$

Since $2N(1-u) < 1$, this shows that, when $m \to \infty$, then $N(1-v_m) \to 0$. Since the v_m belong to a finite set, there exists m such that $N(1-v_m) = 0$, i.e., $v_m = 1$. The relation $v_m = 1$ means that u and v_{m-1} commute, and by prop.9.13 this implies that $v_{m-1} = 1$. By descending induction on m, we obtain $1 = v_{m-2} = v_{m-3} = \cdots = v_1$; hence u and v commute.

Corollary 9.15. *Let U be the set of all $u \in \mathbf{U}_V$ such that $N(1-u) < 1/2$. Let G be a finite subgroup of $\mathbf{U}_V$ and let A be the subgroup of G generated by $G \cap U$. Then A is a normal abelian subgroup of G.*

Proof. That A is normal is clear, since U is stable under the inner automorphisms of $\mathbf{U}_V$, cf. part (2) of prop.9.12. If u, v belong to $G \cap U$, prop.9.14 shows that they commute. Hence A is abelian.

To conclude the proof of th.9.9, it remains to show that $(G : A) \leqslant f(n)$. To do so, we need a packing estimate; it is the topic of the next §.

9.2.5. An upper bound for the number of well-spaced points on a sphere.

Let d be an integer $\geqslant 1$ and let $\mathbf{S}_{d-1}$ be the unit sphere in $\mathbf{R}^d$, i.e., the set of points x with $|x| = 1$, where $|x|$ is the standard euclidean norm $|x| = (\sum x_i^2)^{1/2}$.

Proposition 9.16. *Let δ be a real number, with $0 < \delta < 1$. Let $X \subset \mathbf{S}_{d-1}$ be such that $x, y \in X$, $x \neq y$, implies $|x - y| \geqslant 2\delta$. Then :*

$$|X| \leqslant (\frac{1}{\delta} + 1)^d - (\frac{1}{\delta} - 1)^d. \tag{9.10}$$

Proof. For every $x \in X$, let B_x be the set of y such that $|x - y| < \delta$. The B_x are open balls, and they are disjoint. They are contained in the open ball B_+ made up of the y such that $|y| < 1 + \delta$, and they do not intersect the open ball B_- made up of the y such that $|y| < 1 - \delta$. We thus get :

$$\sum_{x \in X} \mathrm{vol}(B_x) \leqslant \mathrm{vol}(B_+) - \mathrm{vol}(B_-), \tag{9.11}$$

where "vol" means the volume, i.e., the measure for the $dx_1 \cdots dx_d$ measure on $\mathbf{R}^d$. The volume of a spherical ball is proportional to the d-th-power of its radius. Hence $\mathrm{vol}(B_x)$ is independent of x, and we have:

$$\mathrm{vol}(B_+)/\mathrm{vol}(B_x) = (\frac{1+\delta}{\delta})^d \text{ and } \mathrm{vol}(B_-)/\mathrm{vol}(B_x) = (\frac{1-\delta}{\delta})^d \text{ for every } x \in X.$$

If we divide the two sides of (9.11) by $\mathrm{vol}(B_x)$, we obtain (9.10).

9.2.6. End of the proof of th.9.9.

Let G be a finite subgroup of $\mathbf{U}_V = \mathbf{U}_n(\mathbf{C})$, and define $A \subset G$ as in cor.9.15. We have seen that A is an abelian normal subgroup of G. Let $S \subset G$ be a set of representatives of the elements of G/A. If $x, y \in S$ are distinct, then $x^{-1}y \notin A$, hence $N(1 - x^{-1}y) \geqslant 1/2$, i.e., $N(x - y) \geqslant 1/2$ by part (2) of prop.9.12.

Let us now identify the space $M = \mathrm{End}(V) = \mathrm{M}_n(\mathbf{C})$ with $\mathbf{C}^{n^2}$ and thus with $\mathbf{R}^d$, with $d = 2n^2$. This identification transforms the norm $N(x)$ into the euclidean square norm $|x|^2 = x_1^2 + \cdots + x_d^2$ on $\mathbf{R}^d$. Hence we have $|x - y| \geqslant 1/\sqrt{2}$ if x, y are two distinct elements of S. We have $|x| = \sqrt{n}$ by parts (1) and (2) of prop.9.12. Hence the points $x/\sqrt{n}$, $x \in S$, belong to the unit sphere $\mathbf{S}_{d-1}$ of $\mathbf{R}^d$ and the distance between two of these points is $\geqslant 1/\sqrt{2n}$. By applying prop.9.16 with $d = 2n^2$ and $\delta = 1/\sqrt{8n}$, we obtain the desired formula:

$$(G : A) = |S| \leqslant (\sqrt{8n} + 1)^{2n^2} - (\sqrt{8n} - 1)^{2n^2}.$$

9.2.7. Complements.

1. *Optimal $f(n)$*. The value of $f(n)$ given by Frobenius's proof is far from being optimal, see exerc.8. There has been a series of improvements, especially by B. Weisfeiler in the 1980's, culminating in 2007 with M.J. Collins's determination of the optimal value $f_{\text{opt}}(n)$ of $f(n)$, cf. [48]. The proof uses CFSG; it shows that

$$f_{\text{opt}}(n) = (n+1)! \quad \text{for} \quad n \geqslant 71.$$

Note that, because of the inclusion $\mathcal{S}_{n+1} \to \text{GL}_n(\mathbf{C})$, we have $f_{\text{opt}}(n) \geqslant (n+1)!$ for $n > 3$; it is remarkable that there is equality when n is large enough.
The values of $f_{\text{opt}}(n)$ for $1 \leqslant n \leqslant 70$ are also known, cf. [48]; the first six are: $1, 60, 360, 25920, 25920, 6531840$.

2. *Change of ground field.* Jordan's theorem is valid, with the same value of $f(n)$, for the finite subgroups of $\text{GL}_n(k)$, for every field k of characteristic zero. This follows from the *Lefschetz's principle* : observe first that such a subgroup is contained in $\text{GL}_n(k')$, where k' is a subfield of k which is finitely generated over $\mathbf{Q}$, and then use the fact that k' can be embedded in $\mathbf{C}$.
The same result holds when k has characteristic $p > 0$ and the finite group has order prime to p. This is proved by reduction to characteristic zero, using a lifting process similar to the one which allowed us in §4.8.2 to switch from $\mathbf{F}_p$ to $\mathbf{Q}_p$.

3. *The p-part of the index.* Instead of asking that the index $(G : A)$ is small, one may ask about its divisibility properties.
There are two results in that direction : if p is a prime $> 2n+1$ (resp. $> n+1$), then *every finite subgroup G of* $\text{GL}_n(\mathbf{C})$ *has an abelian normal subgroup A such that $(G : A)$ is not divisible by* p (resp. *by* p^2), cf. Feit-Thompson, [54] (resp. Feit, [53]).

4. *Extension to noncompact Lie groups : Zassenhaus's theorem.* Let H be a real Lie group. In [81], Zassenhaus showed that there exists an open subset U of H, containing 1, with the property that every discrete subgroup Γ of H generated by $U \cap \Gamma$ is nilpotent. If H is compact, discrete is the same as finite, and this gives a weaker form of Jordan's theorem (from which one can deduce the full theorem, using exerc.9).

9.3 Exercises

1. Show that every finite subgroup of $\text{GL}_n(\mathbf{Q})$ is conjugate to a subgroup of $\text{GL}_n(\mathbf{Z})$.

2. Show that a maximal finite subgroup of $\text{GL}_2(\mathbf{Q})$ is isomorphic to $\mathcal{D}_4$ or to $\mathcal{D}_6$.
[Hint: prove first that the finite subgroups of $\text{SL}_2(\mathbf{Q})$ are cyclic of order dividing either 4 or 6.]

3. Suppose that n is even. Show that $M(n)/M(n-1)$ is equal to the denominator of b_n/n, where b_n is the n-th Bernoulli number.

4. Show that Minkowski's theorem for n odd implies Minkowski's theorem for $n-1$.
[Hint : use the fact that, if G is a subgroup of $\mathrm{GL}_{n-1}(\mathbf{Q})$, then $\{\pm 1\} \times G$ is a subgroup of $\mathrm{GL}_n(\mathbf{Q})$. Conclude that the order of G divides $\frac{1}{2}M(n)$, which is equal to $M(n-1)$.]

5. (*Blichfeldt-Schur lemma*, [34], n°6.) Let ℓ be a prime number. Let $a \in \mathrm{GL}_n(\mathbf{C})$ be an element of order a power of ℓ such that $\mathrm{Tr}(a^m) \in \mathbf{Q}$ for every $m \in \mathbf{Z}$. Show that there exists an integer y, with $0 \leqslant y \leqslant [\frac{n}{\ell-1}]$, such that $\mathrm{Tr}(a) = n - \ell y$.
[Hint: the eigenvalues of a are roots of unity of ℓ-power order. Moreover, by th.8.38, the $\mathbf{Q}$-rationality hypothesis implies that roots of the same order have the same multiplicity. One may thus decompose $\mathbf{C}^n$ as a direct sum of subspaces, that are stable under a, and where all the eigenvalues have multiplicity 1 and are of the same order ℓ^r. It is enough to prove the formula for $\mathrm{Tr}(a)$ for such a subspace. There are three cases :

   $r = 0$, with $\mathrm{Tr}(a) = 1,\ n = 1,\ y = 0$;

   $r = 1$, with $\mathrm{Tr}(a) = -1,\ n = \ell - 1,\ y = 1$;

   $r \geqslant 2$, with $\mathrm{Tr}(a) = 0,\ n = \ell^{r-1}(\ell - 1),\ y = \ell^{r-2}(\ell - 1)$.]

6. (*Schur's proof of Minkowski's theorem.*) Let ℓ be a prime number. Let A be a finite ℓ-subgroup of $\mathrm{GL}_n(\mathbf{C})$ such that $\mathrm{Tr}(a) \in \mathbf{Q}$ for every $a \in A$. Let $\Omega \subset \mathbf{C}$ be the set of all $\mathrm{Tr}(a)$ for $a \in A - \{1\}$.
a) Let $m = [\frac{n}{\ell-1}]$. Use exerc.5 above to show that every $\omega \in \Omega$ is of the form $n - \ell y$, with $y \in \mathbf{Z}$ and $1 \leqslant y \leqslant m$. In particular, we have $|\Omega| \leqslant m$.
b) Let $P = \prod_{\omega \in \Omega}(n - \omega)$. It is a positive integer, and it is divisible by $|A|$, cf. exerc.11 of chap.8. Use this fact to show that $v_\ell(|A|) \leqslant \sum_\omega v_\ell(n-\omega)$. By a), each $n - \omega$ is of the form ℓy with $1 \leqslant y \leqslant m$. This implies:

$$\sum_{\omega} v_\ell(n-\omega) \ \leqslant\ \sum_{y=1}^{m}(1 + v_\ell(y)) \ \leqslant m + v_\ell(m!).$$

   Hence $v_\ell(|A|) \ \leqslant\ m + v_\ell(m!) = m + \sum_{k \geqslant 1}[m/\ell^k] = M(n, \ell)$.

7. (*Improvement of prop.9.13.*) a) Show that, in prop. 9.13, the hypothesis $N(1-v) < 2$ can be replaced by $N(1-v) < 4$.
[Hint: suppose that $c \neq 1$; show that there exist at least two values of i such that $\lambda_i \neq \lambda_i'$; indeed, if there were only one such i, the multiplicity of λ_i as an eigenvalue of u would be strictly larger than its multiplicity as an eigenvalue of u', contradicting the fact that u and u' are conjugate. Use this fact to obtain $N(1-v) \geqslant 4$, by the method used in the text for proving $N(1-v) \geqslant 2$.]
b) Show that $N(1-v) < 4$ is best possible by constructing an example in $\mathbf{U}_2(\mathbf{C})$ where u, v do not commute, c, u commutent and $N(1-v) = 4$.
[Hint: take $u = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ and $v = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, so that $c = u$.]

8. (*Asymptotic comparison of f and f_{opt}.*) Show that:

$$\log f(n) \sim n^2 \log n \quad \text{and} \quad \log f_{\mathrm{opt}}(n) \sim n \log n \quad \text{for } n \to \infty.$$

   [The notation $a(n) \sim b(n)$ means that $\lim_{n\to\infty} a(n)/b(n) = 1$.]

9. (*A Jordan bound for supersolvable groups.*) Let n be a positive integer; let $ss(n)$ be the maximal order of a supersolvable subgroup of $\mathcal{S}_n$. Let G be finite subgroup of $\mathrm{GL}_n(k)$, where k is a field of characteristic 0; suppose that G is supersolvable. Show that G has an abelian normal subgroup of index $\leqslant ss(n) \leqslant n!$
[Hint: when $k = \mathbf{C}$, use the fact that the linear representations of G are monomial, cf. exerc.12 of chap.8.]
Note that this applies in particular when G is nilpotent.

Chapter 10

Small Groups

We collect here some information about groups that are both small and interesting either by their properties or by their occurence in number theory and algebraic geometry.

We use standard notation. A cyclic group of order n is written C_n. A semidirect product product $A \rtimes B$ is written $A.B$ (the normal subgroup is on the left).

10.1 Small groups and their isomorphisms

10.1.1. Order 6 : $\mathcal{S}_3 \;\simeq\; \mathcal{D}_3 \;\simeq\; \mathrm{GL}_2(\mathbf{F}_2)$.

This is the smallest nonabelian group, and also the smallest Frobenius group; it is a semidirect product $C_3.C_2$. An isomorphism $\mathrm{GL}_2(\mathbf{F}_2) \to \mathcal{S}_3$ is obtained by making the group $\mathrm{GL}_2(\mathbf{F}_2)$ act on the three nonzero elements of $\mathbf{F}_2 \times \mathbf{F}_2$, or, equivalently, on the three points of the projective line $\mathbf{P}_1(\mathbf{F}_2) = \mathbf{F}_2 \cup \{\infty\}$.

10.1.2. Order 12 : $\mathcal{A}_4 \;\simeq\; \mathrm{PSL}_2(\mathbf{F}_3)$.

It is a semidirect product $(C_2 \times C_2).C_3$. The action of $\mathrm{PGL}_2(\mathbf{F}_3)$ on the four points of the projective line $\mathbf{P}_1(\mathbf{F}_3)$ gives an embedding $\mathrm{PGL}_2(\mathbf{F}_3) \to \mathcal{S}_4$ which is an isomorphism since both groups have order 24. This isomorphism maps $\mathrm{PSL}_2(\mathbf{F}_3)$ onto $\mathcal{A}_4$.

10.1.3. Order 12 : $C_3.C_4 = \widetilde{\mathcal{S}_3}$.

This semidirect product is relative to the nontrivial action of C_4 on C_3. It can be generated by two elements x, y with the relations $x^3 = 1, y^4 = 1, yxy^{-1} = x^{-1}$. It is a nonsplit central extension of $\mathcal{S}_3 \;\simeq\; \mathcal{D}_3$ by a group of order 2; this is why it is also denoted by $\widetilde{\mathcal{S}_3}$.

It has an irreducible representation of degree 2 that cannot be realized over its field of characters, which is $\mathbf{Q}$. It is embeddable in $\mathrm{GL}_2(k)$ for every field k of characteristic $p > 3$, see exerc.2.

10.1.4. Order 24 : $\mathcal{S}_4 \simeq \mathrm{PGL}_2(\mathbf{F}_3) \simeq \mathrm{SL}_2(\mathbf{Z}/4\mathbf{Z})/\{\pm 1\} \simeq \mathbf{Aff}^2(\mathbf{F}_2)$.

We have $\mathcal{S}_4 = (C_2 \times C_2).\mathcal{S}_3$. This semidirect decomposition shows that $\mathcal{S}_4$ is isomorphic to the group $\mathbf{Aff}^2(\mathbf{F}_2)$ of automorphisms of the affine $\mathbf{F}_2$-plane.

As for the isomorphism $\mathrm{SL}_2(\mathbf{Z}/4\mathbf{Z})/\{\pm 1\} \simeq \mathcal{S}_4$, it can be obtained by the same method : take for $C_2 \times C_2$ the kernel of $\mathrm{SL}_2(\mathbf{Z}/4\mathbf{Z})/\{\pm 1\} \to \mathrm{SL}_2(\mathbf{F}_2)$, and take for $\mathcal{S}_3$ the subgroup of $\mathrm{SL}_2(\mathbf{Z}/4\mathbf{Z})/\{\pm 1\}$ generated by the images of the matrices $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 2 & 1 \\ 1 & 1 \end{smallmatrix}\right)$.

Another useful description of $\mathcal{S}_4$ is as the *Coxeter group of type* D_3, i.e., the group of permutations, and sign changes (in even number) on three indeterminates, cf. Bourbaki [9], chap.VI, §4.8.

10.1.5. Order 24 : $\mathrm{SL}_2(\mathbf{F}_3) \simeq Q.C_3$, **where** Q **is the quaternion group of order 8.**

It is the only nonsplit central extension of $\mathrm{PSL}_2(\mathbf{F}_3) \simeq \mathcal{A}_4$ by C_2, cf. exerc.3; it is sometimes denoted by $2\mathcal{A}_4$ or by $\widetilde{A_4}$, and it is called the *binary tetrahedral group*. Its semidirect decomposition follows from that of $\mathcal{A}_4$.

This group, as well as $\mathrm{GL}_2(\mathbf{F}_3)$, lifts to a subgroup of $\mathrm{GL}_2(\mathbf{Z}[\sqrt{-2}])$; this fact plays a role in Wiles's proof of Fermat's theorem: it allows him to start the ℓ-adic lifting game with $\ell = 3$.

Note also that $\mathrm{SL}_2(\mathbf{F}_3)$ is the automorphism group of the elliptic curve $y^2 + y = x^3$ over $\mathbf{F}_4$, the isomorphism being given by the action on the 3-division points.

10.1.6. Orders 48 and 96: $\mathrm{SL}_2(\mathbf{Z}/4\mathbf{Z}) \simeq \mathcal{A}_4.C_4$ **and** $\mathrm{GL}_2(\mathbf{Z}/4\mathbf{Z}) \simeq \mathcal{A}_4.\mathcal{D}_4$.

The quotient of $\mathrm{SL}_2(\mathbf{Z}/4\mathbf{Z})$ by $\{\pm 1\}$ is isomorphic to $\mathcal{S}_4$, cf. §10.1.4. The extension

$$1 \to \{\pm 1\} \to \mathrm{SL}_2(\mathbf{Z}/4\mathbf{Z}) \to \mathcal{S}_4 \to 1$$

does not split, but it does over $\mathcal{A}_4$: the eight elements of order 3, the element 1, and the three elements $\left(\begin{smallmatrix} 3 & 2 \\ 0 & 3 \end{smallmatrix}\right), \left(\begin{smallmatrix} 3 & 0 \\ 2 & 3 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 2 \\ 2 & 1 \end{smallmatrix}\right)$, make up a normal subgroup H that is isomorphic to $\mathcal{A}_4$.
The group $\mathrm{SL}_2(\mathbf{Z}/4\mathbf{Z})$ is the semi-direct product of C_4 (generated by $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$) and $H \simeq \mathcal{A}_4$. The diagram:

$$\begin{array}{ccc} \mathrm{SL}_2(\mathbf{Z}/4\mathbf{Z}) & \to & \mathcal{S}_4 \\ \downarrow & & \downarrow \\ C_4 & \to & C_2 \end{array}$$

is *cartesian*, i.e., it describes $\mathrm{SL}_2(\mathbf{Z}/4\mathbf{Z})$ as the product of $\mathcal{S}_4$ and C_4 over C_2, cf. §4.7.

We have similarly $\mathrm{GL}_2(\mathbf{Z}/4\mathbf{Z}) \simeq \mathcal{A}_4.\mathcal{D}_4$, where the dihedral group $\mathcal{D}_4$ is generated by $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 3 \end{smallmatrix}\right)$.

10.1.7. Order 60 : $\mathcal{A}_5 \simeq \mathrm{SL}_2(\mathbf{F}_4) \simeq \mathrm{PGL}_2(\mathbf{F}_4) \simeq \mathrm{PSL}_2(\mathbf{F}_5)$.

It is the smallest nonabelian simple group.

The isomorphism $\mathrm{SL}_2(\mathbf{F}_4) \to \mathcal{A}_5$ follows from the action of $\mathrm{SL}_2(\mathbf{F}_4)$ on the five points of $\mathbf{P}_1(\mathbf{F}_4)$. The isomorphism $\mathrm{SL}_2(\mathbf{F}_4) \to \mathrm{PSL}_2(\mathbf{F}_4) = \mathrm{PGL}_2(\mathbf{F}_4)$ is clear.

The group $\mathrm{PSL}_2(\mathbf{F}_5)$ contains a subgroup isomorphic to $\mathcal{A}_4$, cf. §10.2.2; this subgroup has index 5; this gives a nontrivial action of $\mathrm{PSL}_2(\mathbf{F}_5)$ on a set with 5 elements, hence an embedding into $\mathcal{S}_5$, with image $\mathcal{A}_5$. Hence $\mathrm{PSL}_2(\mathbf{F}_5) \simeq \mathcal{A}_5$.
[Alternative proof: use the uniqueness of the simple groups of order 60, cf. §7.7, th.7.22.]

10.1.8. Order 120 : $\mathcal{S}_5 = \mathcal{A}_5.C_2 \simeq \mathrm{Aut}(\mathcal{A}_5) \simeq \mathrm{PGL}_2(\mathbf{F}_5)$.

The action of $\mathcal{S}_5$ on $\mathcal{A}_5$ by inner automorphisms defines an injection $\mathcal{S}_5 \to \mathrm{Aut}(\mathcal{A}_5)$ which is an isomorphism, cf. chap.1, exerc.18 [1]. As for the isomorphism $\mathcal{S}_5 \simeq \mathrm{PGL}_2(\mathbf{F}_5)$, it follows, for instance, from the fact that $\mathrm{PGL}_2(\mathbf{F}_5)$ contains a subgroup of index 5, namely $\mathcal{S}_4$, cf. §10.2.2.

The group $\mathcal{S}_5$ is also isomorphic to the group of linear and antilinear automorphisms of the projective line $\mathbf{P}_1(\mathbf{F}_4)$; here, an antilinear map means a map such as:

$$z \mapsto (a\bar{z} + b)/(c\bar{z} + d),$$

where $\bar{z}$ is the Galois conjugate of z, i.e., z^2, for $z \in \mathbf{F}_4 \cup \{\infty\}$.

10.1.9. Order 120 : $\mathrm{SL}_2(\mathbf{F}_5) \simeq \widetilde{\mathcal{A}_5}$.

It is the only nonsplit extension of $\mathcal{A}_5$ by C_2, cf. exerc.3; it is called the *binary icosahedral group*. It is embeddable in $\mathrm{GL}_2(\mathbf{F}_q)$ if $q \equiv \pm 1 \pmod 5$, cf. §10.2. It has an irreducible character of degree 2, with values in $\mathbf{Q}(\sqrt{5})$, that is not realizable over that field (nor even over $\mathbf{R}$).

10.1.10. Order 168 : $\mathrm{SL}_3(\mathbf{F}_2) \simeq \mathrm{PSL}_2(\mathbf{F}_7)$.

It is the second-smallest nonabelian simple group; it is the group of automorphisms of Klein's curve of genus 3, with equation $x^3y + y^3z + z^3x = 0$, see e.g. the book [EW].

The isomorphism $\mathrm{SL}_3(\mathbf{F}_2) \simeq \mathrm{PSL}_2(\mathbf{F}_7)$ is a consequence of the uniqueness of the simple groups of order 168, cf. §7.7, th.7.23.

Another method (M. Kneser, [64]) to see this is by using an irreducible 3-dimensional representation of $G = \mathrm{PSL}_2(\mathbf{F}_7)$, cf. chap.8, exerc.26. Corollary 8.50 shows that this representation is realizable over the field of values of its character, which is $\mathbf{Q}(\sqrt{-7})$. Hence G can be embedded in $\mathrm{SL}_3(\mathbf{Q}(\sqrt{-7}))$. Let $\pi = \frac{1+\sqrt{-7}}{2}$; the ring $\mathbf{Z}[\pi]$ is the ring of algebraic integers of $\mathbf{Q}(\sqrt{-7})$ and it is a principal domain; these facts imply that G embeds into $\mathrm{SL}_3(\mathbf{Z}[\pi])$; by reduction mod π, this gives a map $G \to \mathrm{SL}_3(\mathbf{F}_2)$ which is an isomorphism.

Note also that $\{\pm 1\} \times \mathrm{SL}_3(\mathbf{F}_2)$ is a subgroup of $\mathrm{GL}_3(\mathbf{C})$ generated by complex reflections, cf. Bourbaki [9], chap.5, §5, exerc.4.

10.1.11. Order 360 : $\mathcal{A}_6 \simeq \mathrm{PSL}_2(\mathbf{F}_9)$.

Since $9 \equiv -1 \pmod 5$, the group $\mathcal{A}_5$ can be embedded in $\mathrm{PSL}_2(\mathbf{F}_9)$, see §10.2.2. Its index is 6. This gives a nontrivial map : $\mathrm{PSL}_2(\mathbf{F}_9) \to \mathcal{S}_6$, whose image is $\mathcal{A}_6$. This isomorphism also gives an explicit description of the group $\mathrm{Aut}(\mathcal{A}_6)$: it is the semidirect

[1]More generally, $\mathrm{Aut}(\mathcal{A}_n) \simeq \mathcal{S}_n$ if $n \geqslant 4, n \neq 6$, and $\mathrm{Out}(\mathcal{A}_6) \simeq C_2 \times C_2$, see §10.1.11.

product $\mathrm{PGL}_2(\mathbf{F}_9).C_2$, where C_2 acts on $\mathrm{PGL}_2(\mathbf{F}_9)$ through its natural Galois action on $\mathbf{F}_9$ by $z \mapsto z^3$. The group $\mathrm{Out}(\mathcal{A}_6)$ is isomorphic to $C_2 \times C_2$. The three subgroups of index 2 of $\mathrm{Aut}(\mathcal{A}_6)$ are $\mathcal{S}_6$, $\mathrm{PGL}_2(\mathbf{F}_9)$ and another group M_{10} that is the stabilizer of a point in the Mathieu group M_{11}, cf. ATLAS [16], p.4. The first two are semidirect products of C_2 by $\mathcal{A}_6$; the third one, M_{10}, is not; this shows that the extension

$$1 \to \mathcal{A}_6 \to \mathrm{Aut}(\mathcal{A}_6) \to \mathrm{Out}(\mathcal{A}_6) \to 1$$

does not split.
Alternative method. Let $I = \{1, \ldots, 6\}$. Let H be the hyperplane of $\mathbf{F}_3^I$ made up of the (x_i) with $\sum x_i = 0$. The quadratic form $\sum x_i^2$ on H has for kernel the diagonal line D generated by $(1, \ldots, 1)$; it defines a nondegenerate quadratic form q on the 4-dimension $\mathbf{F}_3$-vector space $V = H/D$. The group $\mathcal{S}_6$ acts on H, D, V and fixes q. This gives an embedding : $\mathcal{S}_6 \to \mathrm{O}_{4,q}(\mathbf{F}_3)$, where $\mathrm{O}_{4,q}$ is the orthogonal group of (V, q). We thus obtain an embedding : $\mathcal{A}_6 \to \mathrm{SO}_{4,q}(\mathbf{F}_3)$. The quadratic form q has discriminant -1, which is not a square. This implies that $\mathrm{SO}_{4,q}(\mathbf{F}_3) \simeq \mathrm{SO}_3(\mathbf{F}_9) \simeq \mathrm{PGL}_2(\mathbf{F}_9)$ [we are using here standard properties of quadratic forms in 3 and 4 variables]. This gives an embedding of $\mathcal{A}_6$ into $\mathrm{PGL}_2(\mathbf{F}_9)$ as a subgroup of index 2; since the only such subgroup is $\mathrm{PSL}_2(\mathbf{F}_9)$, we get $\mathcal{A}_6 \simeq \mathrm{PSL}_2(\mathbf{F}_9)$.

10.1.12. Order 720 : $\mathcal{S}_6 \simeq \mathrm{Sp}_4(\mathbf{F}_2)$ **= symplectic group in 4 variables over** $\mathbf{F}_2$.

Here again $I = \{1, \ldots, 6\}$, but we use $\mathbf{F}_2$ instead of $\mathbf{F}_3$. Let $E = \mathbf{F}_2^I$, and let H be the hyperplane made up of the $(x_i)_{i \in I}$ with $\sum x_i = 0$. Let $a(x, y)$ be the alternating bilinear form on H given by $a(x, y) = \sum x_i y_i$; its kernel is the diagonal line D. We thus get a 4-dimensional vector space $V = H/D$ with a nondegenerate alternating form a_V. Every permutation of I gives an automorphism of (V, a_V); this defines an injective homomorphism

$$\epsilon : \mathcal{S}_I \simeq \mathcal{S}_6 \to \mathrm{Aut}(V, a_V) \simeq \mathrm{Sp}_4(\mathbf{F}_2).$$

The order of $\mathrm{Sp}_4(\mathbf{F}_q)$ is $q^4(q^2 - 1)(q^4 - 1)$. For $q = 2$, this gives $720 = 6!$, which is the order of $\mathcal{S}_6$. Hence the injective homomorphism ϵ is an isomorphism.

[*Geometric interpretation.* If we identify I with the set of the six Weierstrass points of a smooth projective curve C of genus 2 in characteristic $\neq 2$, then V is isomorphic to the group of the 2-division points of the Jacobian of C, and the alternating form a_V is the Weil pairing.]

10.1.13. Order 20160 : $\mathcal{A}_8 \simeq \mathrm{SO}_6(\mathbf{F}_2) \simeq \mathrm{SL}_4(\mathbf{F}_2)$.

Let $I = \{1, \ldots, 8\}$. As in §10.1.12, let H be the hyperplane $\sum x_i = 0$ of $\mathbf{F}_2^I$. Let Q be the quadratic form on H defined by $Q(x) = \sum_{i<j} x_i x_j$; its kernel is the diagonal line D. We thus get a 6-dimensional space $V = H/D$ with a nondegenerate quadratic form Q_V. The form Q_V is *hyperbolic*, i.e., isomorphic to $x_1x_2 + x_3x_4 + x_5x_6$; this follows from the existence of 4-dimensional totally isotropic subspaces of H containing D, such as the one defined by the equations :

$$x_1 + x_2 = x_3 + x_4 = x_5 + x_6 = x_7 + x_8, \quad x_1 + x_3 + x_5 + x_7 = 0.$$

Let O_6 denote the corresponding orthogonal group. If q is a power of a prime, the number of elements of $\mathrm{O}_6(\mathbf{F}_q)$ is known to be $2q^6(q^2-1)(q^3-1)(q^4-1)$; in the case $q=2$, it is $40320 = 8!$ The natural action of $\mathcal{S}_8$ on V fixes the quadratic form Q_V; we thus obtain a homomorphism $\mathcal{S}_8 \to \mathrm{O}_6(\mathbf{F}_2)$ which is injective; since these groups have the same order, it is bijective. Hence $\mathcal{S}_8 \simeq \mathrm{O}_6(\mathbf{F}_2)$. This isomorphism maps $\mathcal{A}_8$ onto the unique subgroup of index 2 of $\mathrm{O}_6(\mathbf{F}_2)$, which is the group $\mathrm{SO}_6(\mathbf{F}_2)$ [2].

Let now X be a 4-dimensional vector space over $\mathbf{F}_2$ and let $W = \wedge^2 X$. There is a natural quadratic form $Q_W : W \to \wedge^4 X \simeq \mathbf{F}_2$, given by the formula :

$$Q_W(\sum w_i) = \sum_{i<j} w_i \wedge w_j \quad \text{for} \quad w_i \in W.$$

This form is nondegenerate; it is hyperbolic: if X' is a hyperplane of X, the image of $\wedge^2 X'$ in W is totally isotropic. We thus have $(W, Q_W) \simeq (V, Q_V)$. The group $\mathrm{GL}(X) \simeq \mathrm{SL}_4(\mathbf{F}_2)$ acts on W and fixes Q_W. This defines an injective homomorphism

$$\mathrm{SL}_4(\mathbf{F}_2) \to \mathrm{O}(W,Q)(\mathbf{F}_2) \simeq \mathrm{O}_6(\mathbf{F}_2) \simeq \mathcal{S}_8.$$

Since the order of $\mathrm{SL}_4(\mathbf{F}_2)$ is $\frac{1}{2}8!$, we thus obtain an isomorphism $\mathrm{SL}_4(\mathbf{F}_2) \simeq \mathcal{A}_8$.

[The isomorphism $\mathrm{SL}_4(k) \simeq \mathrm{SO}_6(k)$ holds, not only for $k = \mathbf{F}_2$, but also for any perfect field k of characteristic 2. In characteristic $\neq 2$, it remains valid if one replaces SO_6 by the spin group Spin_6. This reflects the isomorphism between the root systems of types A_3 and D_3.]

10.2 Embeddings of $\mathcal{A}_4$, $\mathcal{S}_4$ and $\mathcal{A}_5$ in $\mathrm{PGL}_2(\mathbf{F}_q)$

In this section, we show how to embed the groups $\mathcal{A}_4$, $\mathcal{S}_4$ and $\mathcal{A}_5$ in $\mathrm{PGL}_2(\mathbf{F}_q)$ and $\mathrm{PSL}_2(\mathbf{F}_q)$.
Note that $\mathrm{PSL}_2(\mathbf{F}_q)$ has index 2 in $\mathrm{PGL}_2(\mathbf{F}_q)$ if q is odd, and is equal to $\mathrm{PGL}_2(\mathbf{F}_q)$ if q is a power of 2.

10.2.1. Characteristic 2.

Proposition 10.1. *Suppose that $q = 2^m$. Then :*
(1) *The group $\mathcal{S}_4$ cannot be embedded in $\mathrm{PGL}_2(\mathbf{F}_q)$.*
(2) *The groups $\mathcal{A}_4$ and $\mathcal{A}_5$ can be embedded in $\mathrm{PGL}_2(\mathbf{F}_q)$ if and only if m is even.*

Proof of (1). The 2-Sylow subgroups of $\mathrm{PGL}_2(\mathbf{F}_q)$ are abelian, and those of $\mathcal{S}_4$ are not.

Proof of (2). The condition "m is even" is equivalent to "$\mathbf{F}_q$ contains a subfield isomorphic to $\mathbf{F}_4$". Since $\mathcal{A}_5 \simeq \mathrm{SL}_2(\mathbf{F}_4) \simeq \mathrm{PGL}_2(\mathbf{F}_4)$, this shows that the condition "m is even" is sufficient. Conversely, suppose that $\mathcal{A}_4$ is embedded in $\mathrm{PGL}_2(\mathbf{F}_q)$. Let X be the 2-Sylow

[2] In characteristic 2, the algebraic group SO_6 is defined as the connected component of the orthogonal group O_6, or, equivalently, as the kernel of the *Dickson invariant* $\mathrm{O}_6 \to \mathbf{Z}/2\mathbf{Z}$, see, e.g., [28], §12.12 (which uses the notation O^+ for our SO_6).

subgroup of $\mathcal{A}_4$; choose a 2-Sylow subgroup S of $G = \mathrm{PGL}_2(\mathbf{F}_q)$ which contains it. Let g be an element of order 3 of $\mathcal{A}_4$; it normalizes X. Since S is abelian, th.2.16 shows the existence of an element of $N_G(S)$ which acts on X as g does; hence $|N_G(S)|$ is divisible by 3; since $|N_G(S)| = 2^m(2^m - 1)$, this means that m is even.

10.2.2. Characteristic $\neq 2$.

Proposition 10.2. *Assume that q is not a power of 2. Then :*
(1) *The group $\mathcal{A}_4$ can be embedded in $\mathrm{PSL}_2(\mathbf{F}_q)$.*
(2) *The group $\mathcal{S}_4$ can be embedded in $\mathrm{PGL}_2(\mathbf{F}_q)$; it can be embedded in $\mathrm{PSL}_2(\mathbf{F}_q)$ if and only if $q \equiv \pm 1 \pmod 8$.*
(3) *The group $\mathcal{A}_5$ can be embedded in $\mathrm{PGL}_2(\mathbf{F}_q)$ if and only if $q \equiv \pm 1 \pmod 5$, in which case it is contained in $\mathrm{PSL}_2(\mathbf{F}_q)$.*

The existence, and the construction, of the embeddings will be given in §10.2.3. The non-existence part is proved as follows :

- If $q \not\equiv \pm 1 \pmod 8$, the order of $\mathrm{PSL}_2(\mathbf{F}_q)$, which is $\frac{1}{2}q(q^2-1)$, is not divisible by 8, hence that group does not contain $\mathcal{S}_4$ whose order is 24.
- If $q \not\equiv \pm 1 \pmod 5$, the order of $\mathrm{PGL}_2(\mathbf{F}_q)$ is not divisible by 5, hence that group does not contain $\mathcal{A}_5$.

Remarks.

1. An easy way to remember prop.10.2 is: " an embedding exists if and only if the order of the first group divides the order of the second group ".

2. By quadratic reciprocity, the congruence conditions on q of (2) and (3) can be restated as follows:

$$q \equiv \pm 1 \pmod 8 \iff \sqrt{2} \in \mathbf{F}_q \qquad \text{and} \qquad q \equiv \pm 1 \pmod 5 \iff \sqrt{5} \in \mathbf{F}_q.$$

When written in this way, prop.10.2 remains valid for every field k of characteristic $\neq 2$, with the extra condition (in characteristic 0) that k contains two elements a, b with $a^2 + b^2 + 1 = 0$; this is how we shall prove it in the next §.

10.2.3. Explicit embeddings of $\mathcal{A}_4$, $\mathcal{S}_4$ and $\mathcal{A}_5$ in characteristic $\neq 2$.

Quaternion preliminaries.

Let us start with a field k of characteristic $\neq 2$, and two elements $a, b \in k$ such that

$$a^2 + b^2 + 1 = 0. \tag{10.1}$$

Note that *such a, b always exist if k is of characteristic $p > 0$*; indeed, they exist if $k = \mathbf{F}_p$: if A (resp. B) is the set of elements that can be written as $-a^2$ (resp. $b^2 + 1$), we have $|A| + |B| = (p+1)/2 + (p+1)/2 > p$, hence $A \cap B \neq \varnothing$.

Let us define $\mathbf{i}, \mathbf{j}, \mathbf{k} \in \mathrm{M}_2(k)$ by :

$$\mathbf{i} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \mathbf{j} = \begin{pmatrix} a & b \\ b & -a \end{pmatrix}, \quad \mathbf{k} = \begin{pmatrix} b & -a \\ -a & -b \end{pmatrix}. \tag{10.2}$$

We have the standard quaternion formulas:

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1, \ \mathbf{ij} = \mathbf{k} = -\mathbf{ji}, \ \mathbf{jk} = \mathbf{i} = -\mathbf{kj}, \ \mathbf{ki} = \mathbf{j} = -\mathbf{ik}. \tag{10.3}$$

They allow us to identify $\mathrm{M}_2(k)$ with the quaternion algebra over k.

The case of $\mathcal{A}_4$.

Let $Q = \{\pm 1, \pm \mathbf{i}, \pm \mathbf{j}, \pm \mathbf{k}\} \subset \mathrm{SL}_2(k)$ be the quaternion group. Let X be the set of the 16 matrices $(\pm 1 \pm \mathbf{i} \pm \mathbf{j} \pm \mathbf{k})/2$. The elements of X normalize Q. The set $Y = Q \cup X$ is a subgroup of $\mathrm{SL}_2(k)$ of order 24, which is the semidirect product of the cyclic group C_3 generated by $(-1 + \mathbf{i} + \mathbf{j} + \mathbf{k})/2$ and Q; it is isomorphic to $\mathrm{SL}_2(\mathbf{F}_3) \simeq \widetilde{\mathcal{A}_4}$, cf. §10.1.5. The image $Y/\{\pm 1\}$ of Y in $\mathrm{PSL}_2(k)$ is isomorphic to $\mathcal{A}_4$. We thus have an explicit form of the embedding claimed in part (1) of prop.10.2.

The case of $\mathcal{S}_4$.

Let $\mathbf{s} = 1 + \mathbf{i}$. We have $\mathbf{s}^2 = 2\mathbf{i}, \mathbf{sis}^{-1} = \mathbf{i}, \mathbf{sjs}^{-1} = \mathbf{k}, \mathbf{sks}^{-1} = -\mathbf{j}$. This shows that $\mathbf{s}$ normalizes Y; let σ be the image of $\mathbf{s}$ in $\mathrm{PGL}_2(k)$; then σ normalizes $Y/\{\pm 1\} \simeq \mathcal{A}_4$. The group generated by $Y/\{\pm 1\}$ and σ is isomorphic to $\mathcal{S}_4$. If $2 = \lambda^2$ with $\lambda \in k$, then $\mathbf{s}/\lambda$ has determinant 1; this shows that $\mathcal{S}_4$ is contained in $\mathrm{PSL}_2(k)$ when 2 is a square in k, as claimed in part (2) of prop.10.2.

The case of $\mathcal{A}_5$.

The method is the same as for $\mathcal{A}_4$: assuming that k contains $\sqrt{5}$, we construct in $\mathrm{SL}_2(k)$ a group S isomorphic to $\mathrm{SL}_2(\mathbf{F}_5)$. This gives a subgroup of $\mathrm{PSL}_2(k)$ that is isomorphic to $\mathrm{SL}_2(\mathbf{F}_5)/\{\pm 1\} \simeq \mathcal{A}_5$.
The construction of S given in Coxeter, [49], is as follows: start with the 8 elements $x + y\mathbf{i} + z\mathbf{j} + w\mathbf{k}$ where $(x, y, z, w) = \frac{1}{2}(0, \pm 1, \pm t, \pm t')$ where t and t' are as in §8.12.2, namely $t = (1 + \sqrt{5})/2$ and $t' = (1 - \sqrt{5})/2$. By permuting these (x, y, z, w) by even permutations, we obtain a set T of $8.12 = 96$ elements. These elements are of order 3 (resp. 4, 5, 6, 10), if their x-coefficient is $-1/2$ (resp. $0, -t/2$ or $-t'/2, 1/2, t/2$ or $t'/2$). We then define S as $S = Y \cup T$, where Y is the group $Q.C_3 \simeq \mathrm{SL}_2(\mathbf{F}_3)$ defined above. See also ATLAS, [16], p.2.

[Note that, by taking $a = \mathbf{i}$, $b = (-1 + t'\mathbf{i} + t\mathbf{j})/2$, $c = (-t' + \mathbf{i} - t\mathbf{k})/2$, we have

$$a^2 = -1, b^3 = 1, c^5 = 1, abc = 1.$$

In PSL_2, this gives the standard presentation of $\mathcal{A}_5$, as generated by two elements of orders 3 and 5 whose product has order 2. Note also that $\mathcal{A}_4$ and $\mathcal{S}_4$ have a similar presentation, with 2,3,5 replaced by 2,3,3 and 2,3,4 respectively, cf. chap.1, exerc.18.
These presentations have a natural interpretation in terms of the 3-point ramification of the covering $\mathbf{P}_1(\mathbf{C}) \to \mathbf{P}_1(\mathbf{C})/G \simeq \mathbf{P}_1(\mathbf{C})$, where G is one of the three groups $\mathcal{A}_4$, $\mathcal{S}_4$ and $\mathcal{A}_5$, acting on the projective line $\mathbf{P}_1(\mathbf{C})$ via the embedding $G \to \mathrm{PGL}_2(\mathbf{C})$.]

10.3 Exercises

1. (*Galois.*) Show that $\mathrm{PSL}_2(\mathbf{F}_q)$ has a subgroup of index q if and only if $q = 2, 3, 5, 7$, or 11.[3]
[Hint: for the "if" part, take a subgroup isomorphic to C_3, $C_2 \times C_2$, $\mathcal{A}_4$, $\mathcal{S}_4$ or $\mathcal{A}_5$. For the "only if" part, use the fact that a subgroup of $\mathrm{PGL}_2(\mathbf{F}_q)$ of order prime to the characteristic is either $\mathcal{A}_4, \mathcal{S}_4, \mathcal{A}_5$ or a subgroup of the triangular group of order dividing $q(q-1)$, or a cyclic subgroup of order dividing $q+1$, cf. Huppert [25], Kap.II, §8; see also Beauville [44] for the analogous result over an arbitrary field.]

2. Let $G = C_3.C_4 = \widetilde{\mathcal{S}_3}$, cf. §10.1.3.
a) Show that G has two irreducible characters of degree 2, with values in $\mathbf{Q}$. One of them comes from the quotient $G/C_2 \simeq \mathcal{S}_3$. Let χ be the other one; it gives a faithful representation of G in $\mathrm{GL}_2(\mathbf{C})$. Show that $\langle \Psi^2\chi, 1\rangle = -1$, hence the representation is not realizable over $\mathbf{Q}$ (and not even over $\mathbf{R}$).
b) Let k be a field. Show that, if its characteristic is $p > 3$, there exist $a, b \in k$ such that $a^2 + b^2 + ab + 1 = 0$.
[Hint: it is enough to prove this when $k = \mathbf{F}_p$; in that case, write the equation as $x^2 + 3y^2 + 1 = 0$ where $x = a + b/2, y = b/2$ and observe that the set of the $x^2 + 1$ has $(p+1)/2$ elements; the same is true for the $-3y^2$; since $(p+1)/2 + (p+1)/2 > p$, these two sets have a nonempty intersection.]
When $p = 3$, show that a, b exist if and only if -1 is a square in k, i.e., if k is an extension of $\mathbf{F}_9$.
c) Let a, b, k be as in b). Show that the matrices $x = \left(\begin{smallmatrix} 0 & -1 \\ 1 & -1 \end{smallmatrix}\right)$ and $y = \left(\begin{smallmatrix} a & b \\ a+b & -a \end{smallmatrix}\right)$ satisfy the relations $x^3 = 1, y^2 = -1, yxy^{-1} = x^{-1}$, hence give an embedding of G into $\mathrm{GL}_2(k)$.
d) Show that G can be embedded in $\mathrm{SL}_2(\mathbf{Z}/4\mathbf{Z})$.
[Hint: use the same matrices as in c), with $a = b = 1$.]
e) Show that G can be embedded in $\mathrm{SL}_2(\mathbf{Z}_p)$ for every prime $p \neq 3$.
[Hint: this is equivalent to proving that G is embeddable in $\mathrm{SL}_2(\mathbf{Z}/p^m\mathbf{Z})$ for every $m \geqslant 1$ if $p \neq 2, 3$ and for every $m \geqslant 2$ if $p = 2$. Do this by using the same matrices as in c); to prove the existence of $a, b \in \mathbf{Z}/p^m\mathbf{Z}$ such that $a^2 + b^2 + ab + 1 = 0$, use induction on m.]
Use the same method to show that G can be embedded in $\mathrm{SL}_2(\mathbf{Z}_3[i])$, where $\mathbf{Z}_3[i]$ means the ring $\mathbf{Z}_3[t]/(t^2+1)$.

3. (*2-central extensions of* $\mathrm{PSL}_2(\mathbf{F}_q)$, *q odd.*)
Let G be a finite group, with a 2-Sylow subgroup S which is dihedral of order $\geqslant 4$. Suppose that all the elements of order 2 of G are conjugate.

a) Show that $|H^2(G, C_2)| \leqslant 2$. Conclude that G has at most one extension by C_2 which does not split, and that, in such an extension, the elements of order 2 of G are images of elements of order 4.
[Hint: let A be a subgroup of order 2 of G, and let $\phi : H^2(G, C_2) \to H^2(A, C_2)$ be the restriction map, cf. §4.2. If $x \in \operatorname{Ker}\phi$, let E_x be the corresponding extension of G by C_2, cf. §4.4. Since $\phi(x) = 0$, this extensions splits over A, hence over all the subgroups of G of order 2, since they are conjugate. Use exerc.4 of chap.4 to show that E_x splits over

[3] In the letter ([57]) to Auguste Chevalier which he wrote the night before his death, Galois states this result when q is a prime. It seems likely that he already knew then (1832) the list of subgroups of $\mathrm{PGL}_2(\mathbf{F}_p)$.

S, hence also over G, by exerc.7 of chap.7. This shows that ϕ is injective. Conclude by using that $H^2(A, C_2) \simeq \mathbf{Z}/2\mathbf{Z}$.]

b) Show that the hypotheses made on G are fulfilled when $G = \mathrm{PSL}_2(\mathbf{F}_q)$, q odd.
[Hint: to show that the elements of order 2 of G are conjugate, prove that every element of order 4 of $\mathrm{SL}_2(\mathbf{F}_q)$ is conjugate to $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$.]

Conclude that $\mathrm{SL}_2(\mathbf{F}_q)$ is the only nonsplit extension of $\mathrm{PSL}_2(\mathbf{F}_q)$ by C_2, up to isomorphism. For $q = 3, 5, 9$, this shows that the groups $\mathcal{A}_4, \mathcal{A}_5, \mathcal{A}_6$ have only one nonsplit extension by C_2 [4].

4. Let σ be the automorphism of $\mathrm{SL}_4(\mathbf{F}_2)$ given by :

$$\sigma(g) = {}^t g^{-1} = \text{inverse of the transpose of } g.$$

Show that the semidirect product $\mathrm{SL}_4(\mathbf{F}_2).\langle 1, \sigma\rangle$ is isomorphic to $\mathcal{S}_8$.

5. (*Hurwitz*, [26], pp.39-40.)
a) Show that there exists a unique homomorphism $\chi_3 : \mathrm{SL}_2(\mathbf{Z}/3\mathbf{Z}) \to \mathbf{Z}/3\mathbf{Z}$ with $\chi_3(\epsilon) = 1$, where $\epsilon = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$.
[Hint: use $\mathrm{SL}_2(\mathbf{Z}/3\mathbf{Z})/\{\pm 1\} \simeq \mathcal{A}_4$, cf. §10.1.2.]
Show that:

$$\chi_3(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)) = ac + cd + bd - bdc^2 = \begin{cases} c(a+d) & \text{if } c \equiv \pm 1 \pmod 3 \\ bd & \text{if } c \equiv 0 \pmod 3). \end{cases}$$

[Hint: let $\phi : \mathrm{SL}_2(\mathbf{Z}/3\mathbf{Z}) \to \mathbf{Z}/3\mathbf{Z}$ be the map defined by the formula above. For every $g \in \mathrm{SL}_2(\mathbf{Z}/3\mathbf{Z})$, show that $\phi(g\epsilon) = \phi(g) + 1$ and that $\phi(g\eta) = \phi(g) - 1$, where $\eta = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$; prove that $\phi(g) = \chi_3(g)$ by writing g as a product $g_1 \cdots g_m$, where each g_i is either ϵ or η.

b) There exists a unique homomorphism $\chi_4 : \mathrm{SL}_2(\mathbf{Z}/4\mathbf{Z}) \to \mathbf{Z}/4\mathbf{Z}$, such that $\chi_4(\epsilon) = 1$, where $\epsilon = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, cf. §10.1.6. Show that:

$$\chi_4(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)) = \begin{cases} c(a+d+1) & \text{if } c \equiv 1 \pmod 2 \\ d(b+c+1) - 1 & \text{if } c \equiv 0 \pmod 2). \end{cases}$$

[Hint: same method as for a).]
Show that $\chi_4 \bmod 2$ is equal to $\mathrm{SL}_2(\mathbf{Z}/4\mathbf{Z}) \to \mathrm{SL}_2(\mathbf{Z}/2\mathbf{Z}) \simeq \mathcal{S}_3 \to \mathbf{Z}/2\mathbf{Z}$.

[The characters χ_3 and χ_4 occur in the formulas describing the action of $\mathrm{SL}_2(\mathbf{Z})$ on the modular forms $\Delta^{1/3}$ and $\Delta^{1/4}$, cf. [26]. More precisely, if $z \in \mathbf{C}$ is such that $\mathrm{Im}(z) > 0$, define $\Delta(z)$ by

$$\Delta(z) = q \prod_{n=1}^{\infty} (1 - q^n)^{24}, \quad \text{where } q = e^{2\pi i z}.$$

We then have, for every $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbf{Z})$, and for $m = 3$ or 4:

$$\Delta^{1/m}\left(\frac{az+b}{cz+d}\right) = w_m^{\chi_m(g)} (cz+d)^{12/m} \Delta^{1/m}(z) \quad \text{where } w_m = e^{2\pi i/m}.$$

(In that formula, $\Delta^{1/m}(z)$ means $e^{2\pi i z/m} \prod_{n=1}^{\infty} (1 - e^{2\pi i n z})^{24/m}$.) This gives a complex analytic definition of χ_3 and χ_4.
For the modular forms interpretation of the subgroups of $\mathrm{SL}_2(\mathbf{Z}/4\mathbf{Z})$, see Lang-Trotter, [32], pp.165-173.]

---

[4] The same is true for all the alternating groups $\mathcal{A}_n$, $n > 3$, as shown by Schur [34], n°17; the corresponding extension is the pull back by $\mathcal{A}_n \to \mathrm{SO}_n$ of the extension $1 \to C_2 \to \mathrm{Spin}_n \to \mathrm{SO}_n \to 1$.

Bibliography

Books

[1] E. Artin & J. Tate, *Class Field Theory*, Benjamin, New York, 1967; revised second edition, A.M.S., 2008.

[2] A. Borel, *Linear Algebraic Groups*, Benjamin, New York, 1969; second enlarged edition, Springer-Verlag, 1991.

[3] N. Bourbaki, *Algèbre. Chapitre* I. *Structures algébriques*, Hermann, 1970; English translation, *Algebra* I, Springer-Verlag, 1998.

[4] —, *Algèbre. Chapitres* IV, V, VI, VII, Masson, 1981; English translation, *Algebra* II, Springer-Verlag, 2003.

[5] —, *Algèbre. Chapitre* VIII. *Modules et anneaux semi-simples*, revised edition, Springer-Verlag, 2011; English translation of the first edition, *Algebra* VIII, Springer-Verlag, 1998.

[6] —, *Algèbre. Chapitre* X. *Algèbre Homologique*, Masson, 1980.

[7] —, *Topologie Générale. Chapitres* I, II, III, IV, Hermann, 1971; English translation, *General Topology. Chapters* 1-4, Springer-Verlag, 1995.

[8] —, *Groupes et Algèbres de Lie. Chapitres* I, II, III, Hermann, 1971-1972; English translation, *Lie Groups and Lie Algebras, Chapters* 1-3, Springer-Verlag, 1989.

[9] —, *Groupes et Algèbres de Lie. Chapitres* IV, V, VI, Hermann, 1968; English translation, *Lie Groups and Lie Algebras, Chapters* 4-6, Springer-Verlag, 2002.

[10] —, *Groupes et Algèbres de Lie. Chapitre* IX, Hermann, 1982; English translation, *Lie Groups and Lie Algebras, Chapters* 7-9, Springer-Verlag, 2005.

[11] K. Brown, *Cohomology of Groups*, Springer-Verlag, 1982.

[12] W. Burnside, *Theory of Finite Groups*, second edition, 1911; reprinted by Dover Publ., 1955.

[13] H. Cartan & S. Eilenberg, *Homological Algebra*, Princeton Univ. Press, Princeton, 1956.

[14] J.W.C. Cassels & A. Fröhlich (edit.), *Algebraic Number Theory*, Acad. Press, 1967; second corrected edition, L.M.S., 2010.

[15] H. Cohen, *Number Theory, Volume II : Analytic and Modern Tools*, GTM 240, Springer-Verlag, 2007.

[16] J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker & R.A.Wilson, *ATLAS of Finite Groups*, Clarendon Press, Oxford, 1985; second corrected edition, 2003.

[17] C.W. Curtis, *Pioneers of Representation Theory : Frobenius, Burnside, Schur and Brauer*, A.M.S., L.M.S., 1999.

[18] W. Feit, *The Representation Theory of Finite Groups*, North Holland Publ., 1982.

[19] F.G. Frobenius, *Gesammelte Abhandlungen*, vol. III, Springer-Verlag, 1968.

[20] W. Fulton & J. Harris, *Representation Theory - a First Course*, Springer-Verlag, 1991.

[21] D. Gorenstein, *Finite Simple Groups - an introduction to their classification*, Plenum Press, New York, 1982.

[22] D. Gorenstein, R. Lyons & R. Solomon, *The Classification of the Finite Simple Groups*, AMS Math. Surveys 40-1, 40-2, ..., 40-6, 1994-2005.

[23] A. Hatcher, *Algebraic Topology*, Cambridge Univ. Press, Cambridge, 2002.

[24] T. Hawkins, *The Mathematics of Frobenius in Context - a journey through 18th to 20th century mathematics*, Springer-Verlag, 2013.

[25] B. Huppert, *Endliche Gruppen I*, Springer-Verlag, 1967.

[26] A. Hurwitz, *Mathematische Werke - I - Funktionentheorie*, Birkhaüser Verlag, Basel, 1962.

[27] I.M. Isaacs, *Character Theory of Finite Groups*, Acad. Press, New York, 1976.

[28] M-A. Knus, A. Merkurjev, M. Rost & J-P. Tignol, *The Book of Involutions*, A.M.S. Colloquium Publications 44, 1998.

[29] S. Lang, *Algebra*, Addison-Wesley, fourth edition, 2007.

[30] —, *Rapport sur la cohomologie des groupes*, Benjamin, 1966; English translation, *Topics in Cohomology of Groups*, Springer Lect. Notes 1625, 1996.

[31] —, *Algebraic Number Theory*, Addison-Wesley, Reading, 1970; second edition, GTM 110, Springer-Verlag, 2000.

[32] S. Lang & H. Trotter, *Frobenius Distributions in* GL_2*-Extensions*, Springer Lect. Notes 504, 1976.

[33] S. Levi (edit.), *The Eightfold Way : The Beauty of Klein's Quartic Curve*, M.S.R.I. Publ. 35 (1998).

[34] I. Schur, *Gesammelte Abhandlungen*, vol. I, Springer-Verlag, 1973.

[35] J-P. Serre, *Corps Locaux*, Paris, Hermann, 1968; English translation, *Local Fields*, Springer-Verlag, GTM 67, 1979.

[36] —, *Cours d'Arithmétique*, Paris, Hermann, 1970; English translation, *A Course in Arithmetic*, Springer-Verlag, GTM 7, 1996.

[37] —, *Représentations Linéaires des Groupes Finis*, fifth edition, Paris, Hermann, 1998; English translation, *Linear Representations of Finite Groups*, Springer-Verlag, GTM 42, 1977.

[38] R.P. Stanley, *Enumerative Combinatorics, volume* I, Cambridge Univ. Press, 1997; new edition with *Errata and Addenda*, 2002.

[39] R.A. Wilson, *The Finite Simple Groups*, Springer-Verlag, 2009.

[40] J. Wolf, *Spaces of Constant Curvature*, McGraw-Hill, 1967; second corrected edition, 1972.

[41] H. Zassenhaus, *The Theory of Groups*, second edition, Vandenhoek and Ruprecht, 1956.

Papers

[42] E. Artin, *Idealklassen in Oberkörpern und allgemeines Reziprozitätsgesetz*, Hamb. Abh. 7 (1929), 46-51; *Coll. Papers*, 159-164.

[43] M.J. Barry & M.B. Ward, *Simple groups contain minimal simple groups*, Publ. Matem. 41 (1997), 411-415.

[44] A. Beauville, *Finite subgroups of* $\mathrm{PGL}_2(K)$, in *Vector Bundles and Complex Geometry*, Contemp. Math. 522, A.M.S. (2010), 23-29.

[45] E. Breuillard, *An exposition of Camille Jordan's original proof of his theorem on finite subgroups of invertible matrices*, notes available on :
http://www.math.u-psud.fr/~breuilla/cour/html.

[46] W. Burnside, *On groups in which every two conjugate operations are permutable*, Proc. LMS 35 (1902), 28-37.

[47] P.J. Cameron & A.M. Cohen, *On the number of fixed-point free elements in a permutation group*, Discrete Math. 106/107 (1992), 135-138.

[48] M. J. Collins, *On Jordan's theorem for complex linear groups*, J. Group Theory 10 (2007), 411-423.

[49] H.S.M. Coxeter, *The binary polyedral groups and other generalizations of the quaternion group*, Duke Math. J. 7 (1940), 367-379.

[50] S. Eilenberg & S. Mac Lane, *Cohomology theory in abstract groups.* II. *Group extensions with a non-abelian kernel*, Ann. Math. 48 (1947), 326-341; *Coll. Works*, 215-240.

[51] P. Erdös & P. Turán, *On some problems of statistical group theory* IV, Acta Math. Acad. Sci. Hungary 19 (1968), 413-435.

[52] B. Fein, W.M. Kantor & M. Schacher, *Relative Brauer Groups* II, Crelle's journal 390 (1981), 39-57.

[53] W. Feit, *Groups that have a faithful representation of degree less than* $p-1$, T.A.M.S. 112 (1964), 287-303.

[54] W. Feit & J.G. Thompson, *Groups which have a faithful representation of degree less than* $(p-1)/2$, Pacific J. Math. 11 (1963), 1257-1262.

[55] —, *Solvability of Groups of Odd Order*, Pacific J. Math. 13 (1963), 775-1029.

[56] P. Flavell, *Finite groups in which two elements generate a solvable group*, Invent. math. 121 (1995), 279-285.

[57] E. Galois, *Lettre à Auguste Chevalier, 29 mai 1832*, J. Math. Pures Appl. 11 (1846), 408-415; *Oeuvres Mathématiques*, Gauthier-Villars, 1897, 25-32.

[58] P. de la Harpe & C. Weber, *Malnormal subgroups and Frobenius groups : basics and examples*, Confluentes Math. 6 (2014), 65-76.

[59] H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischer Zahlkörper. Teil II. Reziprozitätsgesetz*, Jahresbericht der deutschen Mathematiker-Vereinigung 39 (1930), Ergänzungsband VI, 1-204; Physica Verlag, 1965.

[60] G. Higman, *Groups and rings having automorphisms without non-trivial fixed elements*, J. L.M.S. 32 (1957), 321-334.

[61] C. Jordan, *Recherches sur les substitutions*, J. Liouville 17 (1872), 351-367; *Oeuvres* II, 345-361.

[62] —, *Mémoire sur les équations différentielles linéaires à intégrale algébrique*, Crelle's journal 84 (1878), 89-215; *Oeuvres* II, 13-140.

[63] T.M. Keller, *Finite groups have even more conjugacy classes*, Israel J. Math. 181 (2011), 433-444.

[64] M. Kneser, *Über die Ausnahme-Isomorphismen zwischen endlichen klassischen Gruppen*, Abh. Math. Sem. Univ. Hamburg 31 (1967), 136-140.

[65] H.W. Lenstra, Jr & P. Stevenhagen, *Chebotarëv and his density theorem*, Math. Intelligencer 18 (1996), 26-37.

[66] I. Madsen, C.B. Thomas & C.T.C. Wall, *The topological spherical form problem*. II. *Existence of free actions*, Topology 15 (1976), 375-382.

[67] J. Milnor, *Groups which act on* S^n *without fixed points*, Amer. J. Math. 79 (1957), 623-630; *Coll. Papers* II, 97-104.

[68] H. Minkowski, *Zur Theorie der positiven quadratischen Formen*, Crelle's journal 101 (1887), 196-202; *Ges. Abh.* I, n°VI.

[69] P.J. Morandi, *Group Extensions and* H^3, Mathematical Notes, available on the author's home page.

[70] V.P. Platonov, *Theory of algebraic linear groups and periodic groups* (in Russian), Izv. Akad. Nauk SSSR 30 (1966), 573-620; English translation, AMS Translations (2) 1968, 61-110.

[71] L. Pyber, *Finite groups have many conjugacy classes*, J. London Math. Soc. 46 (1992), 239-249.

[72] J-P. Serre, *On a theorem of Jordan*, Bull. A.M.S. 40 (2003), 429-440; reprinted in *Exposés de Séminaires 1950-1999*, Doc.Math. 1, second augmented edition, S.M.F., 2008.

[73] —, *Bounds for the orders of the finite subgroups of $G(k)$*, in *Group Representation Theory* (M. Geck, D. Testerman & J. Thévenaz edit.), C.R.C. Press, Taylor & Francis (2007), 405-450.

[74] J.R. Stallings, *On torsion-free groups with infinitely many ends*, Ann. Math. 88 (1968), 312-334.

[75] L. Stern, *On the equality of norm groups of global fields*, J. Number Theory 36 (1990), 108-126.

[76] R. Swan, *Groups of cohomological dimension one*, J. Algebra 12 (1969), 585-610.

[77] L. Sylow, *Théorèmes sur les groupes de substitutions*, Math. Ann. 5 (1872), 584-598.

[78] J.G. Thompson, *Normal p-complements for finite groups*, Math. Zeit. 72 (1960), 332-354; J. Algebra 1 (1964), 43-46.

[79] —, *Non solvable finite groups all of whose local subgroups are solvable*, I, II, ..., VI, Bull. A.M.S. 74 (1968), 48 (1973), 511-592; Pacific J. Math. 33 (1970), 451-536; *ibid.* 39 (1971), 483-534; *ibid.* 48 (1973), 511-592; *ibid.* 50 (1974), 215-297; *ibid.* 51 (1974), 573-630.

[80] L. Wilson, *The nilpotency class of groups with fixed point free automorphisms*, Groups St. Andrews 2005, vol.2, 685-701, Lect. Notes L.M.S. 340, Cambridge, 2007.

[81] H. Zassenhaus, *Beweis eines Satzes über diskrete Gruppen*, Hamb. Abh. 12 (1938), 289-312.

Topics

- *Algebra* : Bourbaki [3], [4], [5], [6], Lang [29].
- *Simple groups and CFSG* : ATLAS [16], Feit-Thompson [55], Gorenstein [21], Gorenstein-Lyons-Solomon [22], Thompson [79], Wilson [39].
- *Solvable groups, p-groups, Sylow theorems* : Bourbaki [3], Burnside [12], Huppert [25], Lang [29], Sylow [77], Zassenhaus [41].
- *Applications to Galois theory* : Bourbaki [4], Lang [29], Serre [35].

- *Extensions, factor sets, cohomology* : Bourbaki [6], Brown [11], Cartan-Eilenberg [13], Cassels-Fröhlich [14], Eilenberg-Mac Lane [50], Huppert [25], Lang [30], Morandi [69], Serre [35], Zassenhaus [41].
- *Hall theorems* : Huppert [25].
- *Frobenius groups, Frobenius kernels, Frobenius complements, free actions on spheres* : Burnside [46], Feit [18], Huppert [25], Madsen-Thomas-Wall [66], Milnor [67], Thompson [78], Wilson [80], Wolf [40].
- *Transfer* : Artin [42], Huppert [25], Lang [30], Schur [34], Serre [35], Zassenhaus [41].
- *Number Theory* : Artin-Tate [1], Cassels-Fröhlich [14], Cohen [15], Lang [31], Serre [36].
- *Linear representations and characters* : Bourbaki [5], Burnside [12], Feit [18], Frobenius [19], Fulton-Harris [20], Huppert [25], Isaacs [27], Lang [29], Schur [34], Serre [37].
- *Small groups* : ATLAS [16], Beauville [44], Coxeter [49], Kneser [64], Levi [33].
- *Historical aspects* : Burnside [12], Curtis [17], Frobenius [19], Galois [57], Hurwitz [26], Jordan [62], Levi [33], Minkowski [68], Schur [34], Sylow [77].

Index

Ambiguous terminology

a set $\{x, y, z\}$ *of generators* of G : the expression " x is a generator of G " has a clear meaning; it implies that G is cyclic. To say that $\{x, y, z\}$ is a set of generators of G, should then mean that each of them generates G. This is not the case: it usually means that the set $\{x, y, z\}$ generates G.

involution : in group theory, an involution is an element of order 2; elsewhere, it is an element of square 1, which is allowed to be equal to 1 (example: a ring with involution).

natural integer : the number of elements of a finite set, which may be 0; it may also mean (anglo-saxon tradition) an integer $\geqslant 1$.

$\mathbf{N}$: the set of natural integers, in any of the two meanings above, i.e., including or not 0.

positive : for some, it means $\geqslant 0$, and for others, it means > 0.

Index of names



Surveys of Modern Mathematics



10. Finite Groups: An Introduction
Jean-Pierre Serre

9 787040 400984

9. Compressible Flow and Euler's Equations
Demetrios Christodoulou, Shuang Miao

9 787040 390568

8. Lie-Bäcklund-Darboux Transformations
Y. Charles Li, Artyom Yurov

9 787040 390032

7. Introductory Lectures on Manifold Topology: Signposts
Thomas Farrell, Yang Su

9 787040 378306

6. Open Problems and Surveys of Contemporary Mathematics
Lizhen Ji, Yat-Sun Poon, Shing-Tung Yau (Editors)

9 787040 370294

5. Isolated Singular Points on Complete Intersections (Second Edition)
E.J.N. Looijenga

9 787040 348248

4. An Introduction to Rota-Baxter Algebra
Guo Li

9 787040 357004

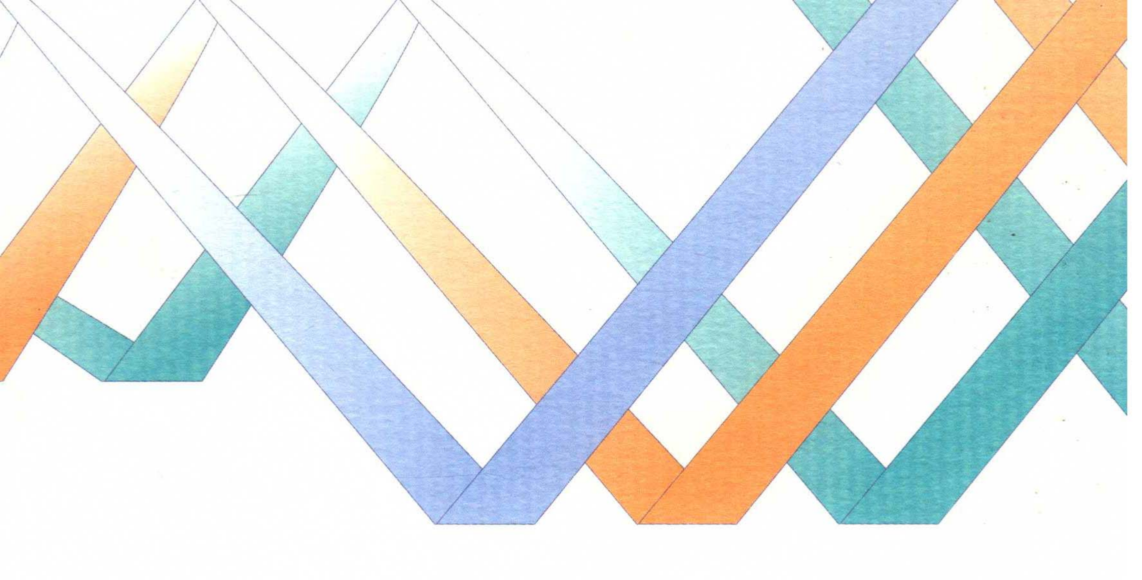
3. Application of Differential Geometry in Influence Analysis
Yat Sun Poon, Wai Yin Poon

9 787040 317091

2. Lie Theory and Representation Theory
Jianpan Wang, Bin Shu, Naihong Hu (Editors)

9 787040 305319

1. Analytic Methods in Algebraic Geometry
Jean-Pierre Demailly



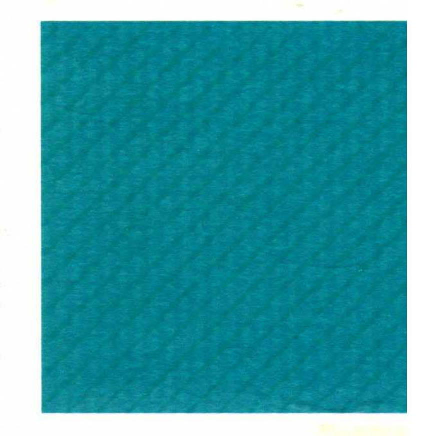
有限群导引

Jean-Pierre Serre

有限群理论以论述简明、论证复杂而引人注目，它以基础的方式应用于数学的多个分支，例如数论等。

本书给出了有限群简明、基础的介绍，以最大限度地服务初学者和数学家。本书共10章，每章都配备了一系列的练习。

让-皮埃尔·塞尔（Jean-Pierre Serre），享有盛誉的法国著名数学家，主要的学术贡献领域是拓扑学、代数几何与数论。他曾获得多项重要的数学奖项，包括1954年的菲尔兹奖、2000年的沃尔夫数学奖与2003年的阿贝尔奖。他被公认为是在数学写作方面世界上最好的数学家之一。







ISBN 978-7-04-044641-8

9 787040 446418 >

学科类别：数学/代数
academic.hep.com.cn

定价 59.00元